Journal of Pioneering Medical Sciences
Received: April 25, 2025 | Accepted: September 21, 2025 | Published: November 05, 2025
Volume 14, Issue 10, Pages 96-119

DOI https://doi.org/10.47310/jpms2025141014

The Internet of Medical Things (IoMT): Analysing Cybersecurity Threats in Connected Healthcare Devices

Blaise Joseph[1*], H. Priya[2], G. Reethikaa[3], S. Rasi[4], Divya P. Chandran[5], Sriragasudha Konda Chandrasekaran[6] and Felyshia Shireen E.S.[7]

[1-7]Saveetha School of Law (SSL), Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai-600077, India

Author Designation: [1]Assistant Professor, [2-7]Student

*Corresponding author: Blaise Joseph (e-mail: blaisejosephin@gmail.com).

©2025 the Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0

Abstract Cybersecurity in Internet of Medical Things (IoMT) devices raises significant concerns within the Indian healthcare system regarding preparedness to handle cyber threats targeting connected medical devices. IoMT implementations demand specialized cybersecurity approaches, yet current regulatory mechanisms lack provisions tailored to their technological complexity. This study explores healthcare stakeholders' perceptions and experiences concerning cybersecurity threats in IoMT implementations, aiming to assess operational gaps and evaluate the need for specialized cybersecurity frameworks. The objective is to understand familiarity with IoMT security challenges and assess opinions on current protective measures. The aim is to examine stakeholder exposure to IoMT cybersecurity techniques and identify demand for structured frameworks. This empirical research is based on 206 structured responses collected via Google Forms using convenient sampling among healthcare stakeholders across demographic groups in India. The independent variables include demographic factors (age, gender, residence, education) and professional experience factors. Dependent variables include threat awareness, perceived component vulnerability, attack frequency perception, trust factors, and support for specialized measures. Data analysis used statistical tools and graphical representations to identify trends and correlations. The research reveals fundamental inadequacies in current IoMT cybersecurity procedures, with software vulnerabilities emerging as the most critical threat across all demographics. Geographic disparities show semi-urban and rural areas facing disproportionate challenges accessing specialized resources. Professional experience creates a paradox where older practitioners recognize limitations more clearly, while younger professionals better understand specialized approaches. Recommendations include immediate implementation of specialized cybersecurity training and standardized protocols differentiating IoMT security from general healthcare IT procedures.

Key Words Internet of Medical Things, Healthcare Cybersecurity, Medical Device Security, Indian Healthcare System, Cybersecurity Threats

INTRODUCTION

The Internet of Medical Things (IoMT) represents a form of interconnected healthcare technology that profoundly challenges conventional cybersecurity mechanisms. Defined broadly, it involves networked medical devices that continuously collect, transmit, and analyse patient data through interconnected systems. Unlike traditional standalone medical equipment that operates in isolation, IoMT devices are frequently vulnerable to cyber threats due to their connectivity, data transmission capabilities, and integration with broader healthcare networks. These devices are typically designed with functionality prioritized over security, often with inadequate encryption protocols and limited security updates. These characteristics make IoMT cybersecurity particularly challenging, as attackers may exploit multiple vulnerabilities simultaneously, and the devices may operate across different healthcare systems or span several years without security patches. In countries where healthcare digitization has advanced rapidly, such threats are approached through specialized cybersecurity frameworks and regulatory oversight. However, in India, the healthcare technology framework continues to apply generic cybersecurity approaches to all medical devices, regardless of connectivity risks or data sensitivity. This absence of IoMT-specific cybersecurity protocols impairs both the protection and secure deployment of connected medical devices.

India's encounter with healthcare cybersecurity threats is not a recent phenomenon. Cases such as the 2017 WannaCry ransomware attack affecting healthcare institutions globally, data breaches in Indian hospital systems,

and the growing incidents of medical device vulnerabilities reveal that this country faces significant challenges in securing connected healthcare technologies. These incidents also expose the limitations of India's healthcare cybersecurity approach, which tends to treat each device as an isolated system rather than part of an interconnected ecosystem. Security assessments are often fragmented, lacking coordination between healthcare institutions and cybersecurity specialists. The National Health Authority (NHA), while promoting digital health initiatives, does not classify or track IoMT-specific cybersecurity incidents as a distinct category, thereby failing to recognize patterns early or support proactive security interventions. In contrast, international agencies like the Food and Drug Administration (FDA) in the United States employ frameworks such as cybersecurity guidelines for medical devices and mandatory security assessments to analyse device vulnerabilities, ensure secure deployment, and predict potential attack vectors. The gap between global best practices and India's healthcare cybersecurity approach highlights an urgent need for reform.

This research aims to critically examine the adequacy of India's current cybersecurity framework in handling IoMT devices, with particular focus on the technological and behavioural dimensions of cyber threats. It aims to investigate whether the absence of specialized IoMT cybersecurity protocols is contributing to security vulnerabilities, inadequate threat detection, or improper risk assessment in connected healthcare environments. Furthermore, the study attempts to gauge the perceptions and experiences of healthcare stakeholders—those who implement and manage IoMT systems in clinical settings—through structured analysis. Their insights are essential for determining whether there is operational and institutional readiness for introducing dedicated cybersecurity frameworks that incorporate threat assessment, vulnerability management, and incident response protocols within healthcare technology deployment.

Cybersecurity in healthcare technology is not a new phenomenon in human history. The earliest known attempts to secure medical information date back to traditional paper-based systems with physical access controls and confidentiality protocols. These approaches evolved significantly with the digitization of healthcare in the late 20th century, incorporating database security, network firewalls, and access authentication systems. Modern healthcare cybersecurity became institutionalized in the 2000s with regulations like HIPAA in the United States, which established standards for protecting patient health information. The development of specialized frameworks for medical device security emerged through initiatives by organizations like the FDA and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Empirical validation for IoMT cybersecurity as a critical healthcare component came through academic research and real-world incidents; for instance, studies have demonstrated that connected medical devices face significantly higher security risks compared to standalone equipment. However, in India, IoMT cybersecurity remains largely theoretical. As various healthcare technology reports indicate, specialized cybersecurity measures for connected medical devices have found limited application in actual healthcare deployments and are neither mandated by regulations nor supported by institutional frameworks.

The Information Technology Act of 2000, and subsequent healthcare digitization policies provide frameworks for data protection and cybersecurity in India's digital infrastructure. While these regulations offer mechanisms for data privacy, network security, and digital authentication, they remain structurally insufficient for addressing IoMT-specific vulnerabilities. Healthcare technology deployment guidelines focus on interoperability, data exchange standards, and digital health record management, yet none explicitly acknowledge the unique cybersecurity challenges posed by interconnected medical devices operating in clinical environments. There is also no provision for specialized cybersecurity assessments or mandatory security protocols for IoMT devices, unless related to general data protection requirements. This regulatory gap becomes problematic in IoMT implementations, where device vulnerabilities can directly impact patient safety and healthcare delivery. Currently, Indian healthcare institutions must rely on generic cybersecurity measures, limited technical expertise, and ad-hoc security implementations. There is no regulatory guideline for IoMT-specific threat assessment, nor is there institutional support for integrating cybersecurity expertise into healthcare technology management. This systemic inadequacy, particularly when IoMT adoption is accelerating globally, points to a critical research gap.

The Indian healthcare and technology systems face multiple challenges in adapting to IoMT cybersecurity requirements. One of the foremost issues is the lack of trained cybersecurity specialists with healthcare technology expertise within medical institutions. Without access to specialized professionals, healthcare administrators are unable to assess device vulnerabilities, implement appropriate security controls, or respond effectively to cyber incidents. Furthermore, India lacks centralized cybersecurity monitoring systems specifically designed for healthcare environments, similar to specialized health sector cybersecurity centres in developed countries. This absence of integrated security monitoring prevents healthcare institutions from detecting threats early or coordinating responses across different facilities. Additionally, there is no regulatory flexibility to allow for specialized cybersecurity protocols tailored to different types of medical devices or clinical environments. Medical colleges and healthcare administration programs do not offer structured training in healthcare cybersecurity or IoMT security management as part of their curriculum, creating knowledge gaps among healthcare professionals. Interdisciplinary collaboration between healthcare institutions and cybersecurity organizations is virtually non-existent. Research on

healthcare cybersecurity frameworks and IoMT security protocols suggests that systematic approaches to device security assessment and threat monitoring could significantly improve protection levels. The Indian healthcare system, however, lacks both the regulatory mandate and institutional capacity to implement such specialized security measures.

The popularization of digital health technologies and increased awareness of cybersecurity risks have led to growing concern about IoMT security among healthcare stakeholders in India. Healthcare digitization initiatives, telemedicine expansion, and the adoption of connected medical devices have familiarized healthcare professionals with concepts like device vulnerabilities, data encryption, and network security. This growing awareness has sparked discussions within healthcare management and medical technology communities across the country. Yet, the practical implementation of comprehensive IoMT cybersecurity measures remains limited. Most healthcare institutions lack the technical expertise, financial resources, or regulatory guidance needed to implement specialized security protocols for connected medical devices. In academia, the study of healthcare cybersecurity and IoMT security is gaining attention through research initiatives and professional development programs. However, these efforts remain optional and are not integrated into mainstream healthcare technology management practices. Without systematic incorporation of IoMT cybersecurity into healthcare technology deployment and management procedures, the insights from these initiatives remain underutilized.

Comparing with countries like the United States, United Kingdom, and Canada, IoMT cybersecurity is not just a theoretical concern but a legally mandated requirement with established implementation frameworks. The FDA's cybersecurity guidelines for medical devices have been operational since 2014 and require manufacturers to demonstrate security measures throughout the device lifecycle. The U.K.'s National Health Service (NHS) has implemented comprehensive cybersecurity frameworks specifically for healthcare technology, including mandatory security assessments for connected medical devices. In Canada, healthcare cybersecurity standards are integrated into provincial health technology procurement and deployment processes. These systems are effective because regulatory frameworks support specialized security measures, and healthcare institutions have access to trained cybersecurity professionals with healthcare technology expertise. In contrast, Indian healthcare institutions rely primarily on generic cybersecurity measures without specialized protocols for medical devices. IoMT cybersecurity is neither mandated by regulations nor supported by institutional frameworks. Unless India develops comprehensive healthcare, cybersecurity policies and builds specialized technical capacity, it risks significant vulnerabilities in its expanding digital health infrastructure.

IoMT devices pose unique cybersecurity challenges that extend beyond traditional information technology security concerns. When healthcare institutions deploy connected medical devices without adequate security protocols, they create vulnerabilities that can directly impact patient safety, compromise sensitive health data, and disrupt critical healthcare services. The interconnected nature of IoMT systems means that a security breach in one device can potentially affect entire healthcare networks, creating cascading risks that traditional cybersecurity approaches are not designed to address. The Indian healthcare framework, while advancing rapidly in digital health adoption, remains inadequately prepared to secure IoMT implementations in a manner that ensures patient safety and data protection.

This research, therefore, undertakes a comprehensive approach to understanding IoMT cybersecurity challenges in the Indian healthcare context. Through systematic analysis of cybersecurity threats, assessment of current security measures, and evaluation of stakeholder perceptions, the study aims to develop evidence-based recommendations for enhancing IoMT cybersecurity in Indian healthcare systems. The research objectives focus on identifying key cybersecurity threats, assessing their potential impact on patient safety and data privacy, evaluating current security frameworks, and proposing strategies for improving IoMT cybersecurity. Through this comprehensive examination, the study seeks to contribute to the development of more secure, resilient, and patient-safe IoMT implementations that can support India's healthcare digitization goals while maintaining the highest standards of cybersecurity and patient protection.

Objectives

- To identify the key cybersecurity threats affecting Internet of Medical Things (IoMT) devices
- To assess the potential impact of these threats on patient safety and healthcare data privacy
- To evaluate the effectiveness of current security measures and regulatory frameworks for IoMT
- To recommend strategies for enhancing the cybersecurity of connected healthcare devices

Research Question

- What are the primary cybersecurity threats facing IoMT devices in modern healthcare systems?
- How effective are current technical and regulatory measures in mitigating cybersecurity risks in IoMT?

LITERATURE REVIEW

Joyia *et al.* [1], The objective of the paper is to explore and present the contributions of the Internet of Things (IoT), specifically the Internet of Medical Things (IoMT), in the healthcare domain, focusing on how IoMT enhances the accuracy, reliability, and productivity of medical devices. The methodology is based on a review of existing research contributions, applications, and emerging challenges related to IoT integration in medical services. The paper emphasizes the role of IoT in digitizing healthcare by interconnecting medical resources and services, and provides a detailed account of the applications and limitations within the IoMT

framework. The findings highlight the significant potential of IoT to transform the healthcare industry and underscore the importance of understanding both past contributions and current challenges to facilitate further research and practical advancements in the field.

Gatouillat [2], the objective of the paper is to enhance the understanding of how the Internet of Medical Things (IoMT)—the interconnection of communication-enabled medical devices within broader health networks—can be improved in terms of reliability, safety, and security. The methodology involves a comprehensive literature review of recent research contributions, particularly those that apply formal methodologies from the cyber-physical systems (CPS) community to address critical challenges in IoMT. The findings highlight the practical benefits of democratizing medical devices for both patients and healthcare providers, while also acknowledging that significant challenges remain. The paper concludes by identifying unexplored research directions and emerging trends, offering insights into potential solutions for addressing currently uncharted issues in the field of IoMT.

Hatzivasilis *et al.* [3], The objective of the paper is to explore the intersection of the Internet of Medical Things (IoMT) and the Circular Economy (CE) in the healthcare sector, with a particular focus on identifying and addressing the growing security and privacy risks associated with the increasing use of mobile, wearable, and telemedicine devices. The methodology involves a comprehensive review of current IoMT implementations in CE-based healthcare services—such as remote sensing and e-visits—while analysing the emerging threats posed by trends like Bring Your Own Device (BYOD) and the reuse of devices by multiple stakeholders. The findings highlight that as IoMT devices handle highly sensitive medical data, they are becoming prime targets for ransomware and other cyberattacks, yet medical users and vendors often underinvest in security measures. The paper proposes a set of core security and privacy controls as a best-practices guide to help secure IoMT systems within CE frameworks, emphasizing that known vulnerabilities can be effectively mitigated when appropriate and relevant safeguards are implemented.

Nkomo and Brown [4], the objective was to create a hybrid cybersecurity framework for Internet of Medical Things (IoMT) that addresses the lack of specific standards tailored to IoMT security and helps safeguard patient safety while maintaining the security and privacy of patient information, particularly useful for the UK healthcare industry as it moves towards full adoption of IoMTs. The methodology involved extending the NIST cybersecurity framework Version 1.1 to develop a hybrid approach that addresses the specific security challenges of IoMT, recognizing that existing cybersecurity frameworks such as ISO 27000 x series, NIST CSF 2018, or COBIT are either outdated or lack the required approach to protect IoMT technology. The findings demonstrated that despite IoMT benefits in healthcare, achieving robust security and privacy remains a huge challenge due to increased information flow from IoMT endpoints and applications that expands the risk landscape, with risks including potential harm to patient safety, compromise to patient health information, and unauthorized device access; however, the proposed hybrid framework addresses these concerns while acknowledging that with proper security measures in place, IoMTs can deliver more benefits than risk, particularly in addressing GDPR compliance issues in the domain of consent and providing guidelines for implementing security controls in IoMT environments.

Vishnu *et al.* [5], The objective of the paper is to provide an overview of the Internet of Medical Things (IoMT) and its transformative role in the healthcare sector, focusing on areas such as remote healthcare monitoring, ingestible sensors, mobile health, smart hospitals, and enhanced chronic disease treatment. The methodology adopted is a descriptive and analytical review of existing technologies, relying on secondary data to examine the development of smart sensors, smart devices, and advanced communication protocols that enable seamless interconnectivity among medical devices. The findings highlight that IoMT facilitates real-time, automated health monitoring and diagnosis without human intervention, improving the accuracy, efficiency, and personalization of healthcare services. Applications such as wearable and ingestible sensors, remote diagnostics, and smart healthcare infrastructures significantly enhance patient care and chronic disease management.

Yaacoub *et al.* [6], The objective of the paper is to address the growing challenges faced by traditional healthcare systems, particularly in light of increasing patient loads, by emphasizing the potential of the Internet of Medical Things (IoMT) to enhance accuracy, reliability, and efficiency in healthcare delivery. The methodology involves a detailed review and classification of existing IoMT security and privacy issues, along with an analysis of current cryptographic and non-cryptographic solutions based on their computational complexity and resource requirements. The paper highlights the trade-off between security and system performance in the evolving digital healthcare (v4.0) era, and discusses the need for optimized security approaches such as lightweight cryptographic algorithms and resource-efficient protocols. The findings stress the critical importance of implementing appropriate security measures and training to protect IoMT systems from cyber threats. The authors propose a five-layered security framework incorporating intrusion detection/ prevention systems and dynamic shadow honeypots to mitigate known attacks and safeguard patient privacy, while acknowledging that zero-day attacks remain a significant unresolved challenge.

Thomasian and Adashi [7], the objective was to analyse the robustness of existing policy measures in securing Internet of Medical Things (IoMT) technologies, focusing on the US regulatory ecosystem including industry frameworks, public-private partnerships, and transparency

initiatives. The methodology involved a qualitative review of medical cybersecurity literature, collecting federal and international legal documents, policy reports, industry frameworks, cyberbreach analyses, and scientific journal articles. The findings revealed that current regulatory guidance emphasizes device identification, legacy device management, enhanced physical security, and breach detection, with recent trends strengthening federal enforcement authority for baseline security safeguards; however, significant gaps exist requiring additional guidance for retrofitted IT infrastructures, edge-to-cloud interfaces, off-the-shelf components, and emerging threats like novel attack vectors, autonomous cyber-physical systems, and quantum computing, with recommendations for awareness interventions and security hygiene measures to empower end users and facilitate incident response while ensuring IoMT benefits don't compromise patient safety and privacy.

Saheed and Arowolo [8], the objective was to demonstrate how a deep recurrent neural network (DRNN) and supervised machine learning models (random forest, decision tree, KNN, and ridge classifier) can be utilized to develop an efficient and effective intrusion detection system (IDS) in the Internet of Medical Things (IoMT) environment for classifying and forecasting unexpected cyber threats. The methodology involved preprocessing and normalization of network data, followed by feature optimization using a bio-inspired particle swarm algorithm, and conducting a thorough evaluation of experiments using DRNN and other supervised machine learning models on standard intrusion detection datasets. The findings established through rigorous testing that the proposed supervised machine learning model outperforms existing approaches with an accuracy of 99.76% in detecting and classifying cyber threats in IoMT environments, demonstrating effectiveness against security challenges such as remote hijacking, impersonation, denial of service attacks, password guessing, and man-in-the-middle attacks that threaten the IoMT ecosystem.

Elsayeh *et al.* [9], The objective was to develop a combined security architecture that fuses standard architecture with new blockchain technology to ensure secure data transmission and storage in Internet of Medical Things (IoMT) systems, particularly for healthcare providers like private clinics, hospitals, and healthcare organizations that require secure data sharing. The methodology involved examining the innovation behind blockchain technology and then proposing an IoMT-based security architecture utilizing blockchain to guarantee the security of information transmission between associated nodes, developing a method to collect vital signs data from IoMT and connected devices using standard in-depth strategy combined with blockchain for secure and decentralized data storage and retrieval within a closed system suitable for healthcare environments. The findings from experimental analysis showed that the proposed scheme presents non-significant overhead while bringing major advantages to meet standard security and privacy requirements in IoMT, demonstrating that blockchain's tamper-resistant digital ledger capabilities can provide peer-to-peer communication and facilitate secure communication between non-trust individuals, effectively addressing the challenge of keeping large amounts of continuously developing IoMT data secure while enabling safe transfer to third parties such as cloud systems for future use.

Razdan and Sharma [10], the objective of the paper is to explore the integration of Internet of Things (IoT) with medical devices, forming the Internet of Medical Things (IoMT), and to present how this integration can enhance patient comfort, reduce costs, and enable faster and more personalized healthcare. The methodology involves a conceptual analysis beginning with an introduction to IoMT, followed by the development of an IoMT architectural model. It then maps existing healthcare operations onto this architecture and investigates the role of emerging technologies—such as Physically Unclonable Functions (PUF), Blockchain, Artificial Intelligence (AI), and Software-Defined Networking (SDN)—in addressing key challenges like security, privacy, accuracy, and performance in e-healthcare. The paper includes three illustrative case studies: PUF-based authentication, AI-enabled SDN-assisted e-healthcare, and a Blockchain-assisted patient-centric system. The findings suggest that these innovative technological solutions have significant potential to accelerate the development and effectiveness of IoMT infrastructure in line with evolving healthcare needs.

Kakhi *et al.* [11], The objective of the paper is to explore the integration of Artificial Intelligence (AI) with the Internet of Medical Things (IoMT) to enhance the efficiency and cost-effectiveness of healthcare services, particularly in the context of remote medical care. The methodology involves a comprehensive literature review of recent research articles, technological developments, and hardware requirements related to AI-powered IoMT solutions. The paper also examines wearable medical devices (WMDs), classifying them based on technology and analysing their market share and projected growth for the first time. The findings underscore AI's critical role in enabling remote disease diagnosis and chronic disease monitoring through IoMT, leading to lower healthcare costs and improved service quality. Additionally, the paper presents a categorized overview of common AI applications in IoMT, outlines the benefits and challenges of implementing such technologies, and concludes with future research directions.

Hasan *et al.* [12], The objective was to identify threats that could undermine the integrity, privacy, and security of Internet of Medical Things (IoMT) systems, and explore novel blockchain-based approaches that can help improve the confidentiality of IoMT networks, particularly in the context of 5G-based AI technology that can revolutionize healthcare and lifestyle perceptions. The methodology involved reviewing recent advancements in IoT embedded systems, wireless networks, and biosensors that have assisted in the rapid development of implanting wearable sensors, as well as examining IoMT applications as an ecosystem of connected clinical systems, computing

systems, and medical sensors aimed at improving healthcare service quality. The findings discovered that IoMT is vulnerable to various types of attacks including denial of service (DoS), malware, and eavesdropping attacks, and is exposed to vulnerabilities related to security, privacy, and confidentiality; however, despite these multiple security threats, novel cryptographic techniques such as access control, identity authentication, and data encryption can help improve the security and reliability of IoMT devices, with blockchain-based approaches showing promise for enhancing network confidentiality.

Huang *et al.* [13], The objective of the paper is to provide a comprehensive review of the Internet of Medical Things (IoMT), highlighting its conceptual foundation, deployment domains, technologies, and diverse medical applications such as smart hospitals, remote health monitoring, disease diagnosis, and infectious disease tracking. The methodology involves a theoretical and literature-based review, supported by over one hundred representative references and practical examples, to analyse how smart devices like wearable sensors and medical instruments collect and transmit health data for enhanced medical decision-making. The findings emphasize that IoMT significantly contributes to the development of connected healthcare systems by enabling efficient data collection, processing, and analysis, ultimately improving patient care. The paper also presents a forward-looking discussion on current challenges and future directions, aiming to assist a broad audience—including researchers, healthcare administrators, policymakers, and industry newcomers—in understanding and advancing IoMT implementation.

Ameen *et al.* [14], The objective was to summarize previous research in the Internet of Medical Things (IoMT) and discuss the roles of artificial intelligence (AI), blockchain (BC), and cybersecurity in IoMT, as well as examine the problems, opportunities, and research directions in this field through a comprehensive literature review. The methodology involved conducting a comprehensive literature review to analyse the integration of AI, BC, and cybersecurity technologies in IoMT systems, focusing on their roles, challenges, and potential applications in healthcare. The findings revealed that while combining blockchain technology with artificial intelligence can create a safer IoMT environment to address privacy and security challenges faced by healthcare centres and patients due to cyberattack vulnerabilities, current systems remain costly and still suffer from security and privacy problems; the review identified integration schemes of AI, BC, and cybersecurity technologies that can support the development of new decentralized healthcare systems, while also documenting the strengths and weaknesses of these technologies along with the datasets they utilize.

Alkatheiri and Alghamdi [15], the objective was to propose a Blockchain-Assisted Cybersecurity (BCCS) system for the Internet of Medical Things (IoMT) in the healthcare industry to maintain all data safely and securely within the rapidly growing big-data platform, utilizing blockchain's decentralized digital ledger capabilities to enable end-to-end communication and provide interaction between untrustworthy persons in healthcare environments. The methodology involved using a conventional in-depth approach combined with blockchain technology to create a procedure for collecting medical information from IoMT and integrated devices, utilizing blockchain to record and extract accumulated information in a secure and distributed manner within a closed environment suitable for healthcare professionals such as nursing homes, hospitals, and healthcare industry where data exchange is needed. The findings from experimental outcomes demonstrated that the proposed BCCS system achieved a high security rate of 99.8% and the lowest latency rate of 4.3% compared to traditional approaches, with an overall reliability rate of 99.4%, effectively addressing the critical need to maintain IoMT data safely and securely while facilitating monitoring and checking of patient medical information before transferring data to cloud networks for future use.

Yazid [16], the objective was to identify and analyse the key cybersecurity and privacy issues associated with the Internet of Medical Things (IoMT) and provide recommendations for healthcare providers and device manufacturers to address these issues, recognizing that increased connectivity brings increased risk of cybersecurity and privacy problems despite IoMT's potential to revolutionize healthcare through real-time health information, remote monitoring, and improved treatment options. The methodology involved conducting a research study that examined various cybersecurity risks and vulnerabilities in IoMT systems, analysing data breaches, device vulnerabilities, encryption gaps, insider threats, and regulatory compliance challenges to develop comprehensive recommendations for risk mitigation. The findings identified five significant cybersecurity risks: data breaches involving sensitive medical data valuable to hackers for identity theft and insurance fraud, vulnerable devices not designed with security in mind that hackers can exploit, lack of encryption leaving data vulnerable to interception, insider threats from healthcare employees who may accidentally or intentionally leak sensitive data, and regulatory compliance challenges with HIPAA and GDPR that can result in fines and legal penalties; the study recommended implementing strong authentication and access controls, using encryption technologies like SSL and TLS, regularly updating and patching devices, training employees on cybersecurity best practices, implementing role-based access control, conducting security awareness training, using auditing and monitoring tools, and prioritizing cybersecurity and regulatory compliance in the design, implementation, and maintenance of IoMT systems.

Vijayakumar *et al.* [17], The objective was to develop a resilient cyber-attack detection system in the Internet of Health Things (IoHT) environment for mitigating security risks and preventing IoHT devices from becoming exposed to cyber-attacks, recognizing that IoHT devices and

applications have become extensively vulnerable to cyber-attacks due to their small size and heterogeneous nature, which is doubly significant in healthcare domain applications. The methodology involved building a deep neural network-based cyber-attack detection system by employing artificial intelligence on the latest ECU-IoHT dataset to uncover cyber-attacks in the IoHT environment, utilizing deep learning techniques for anomaly detection to address the growing vulnerability of rapidly expanding IoHT devices and applications. The findings demonstrated that the proposed deep neural network system achieved superior performance with an average accuracy of 99.85%, an average area under receiver operator characteristic curve of 0.99, and a false positive rate of 0.01, with experimental results showing that the proposed system attains a higher detection rate than existing methods, effectively addressing the critical need for cybersecurity in IoHT devices that provide electronic healthcare services and have the capacity to increase the quality of patient care in day-to-day life.

Bughio *et al.* [18], The objective was to address a significant gap in existing literature regarding a comprehensive ontology for vulnerabilities in medical IoT devices by proposing a fundamental domain ontology named MIoT (Medical Internet of Things) ontology, focusing on cybersecurity in IoMT (Internet of Medical Things), particularly in remote patient monitoring settings, to establish semantic interoperability among medical devices and secure IoMT assets from vulnerabilities and cyberattacks. The methodology involved utilizing the knowledge engineering methodology outlined in Ontology Development 101 along with the structured life cycle to develop the MIoT ontology, defining key concepts and relationships to understand and analyse the complex network of information within IoMT, capturing essential key terms and security-related entities, deriving a conceptual model from the MIoT ontology, and validating it through a case study. The findings demonstrated that the MIoT ontology successfully establishes semantic interoperability among medical devices, making it easier to understand and analyse IoMT networks while addressing data security and interoperability challenges faced by IoMT systems that integrate medical devices for real-time data analysis and transmission, with the research also outlining a roadmap for future research and highlighting potential impacts on security automation in healthcare applications.

Ksibi *et al.* [19], The objective was to address the urgent need for smart and efficient security solutions in Internet of Medical Things (IoMT) environments by conducting an in-depth study of security concerns and introducing a framework to enhance trustworthiness and support decision making within IoMT environments, recognizing that existing traditional models are no longer convenient and unsuitable to address the various security risks created by the complexity and heterogeneity of data and technology in IoMT communications. The methodology involved reviewing popular risk assessment and management approaches and discussing their suitability to the IoMT context, identifying main shortcomings inherent to complex architecture, lack of automation, and numerous stakeholders with different security needs and skills, then developing a solution that relies on a fine-grained approach for managing associated risks with regard to different areas of focus and common risk factors using a Machine Learning (ML)-based anomaly detection model and a hybrid Risk Assessment (RA) model to evaluate cumulative IoMT risk. The findings demonstrated that the proposed framework achieved competitive results compared to state-of-the-art ML models for detecting intrusions in IoT/IoMT systems, obtaining an accuracy rate of 100% with some algorithms, effectively addressing security and privacy problems raised by Connected Medical Devices (CMD) and the exploitation of crucial vulnerabilities by malicious users in IoMT applications, networks, and devices, with a use case presented to highlight the efficiency of the proposal in enhancing security for smart technologies integrated into medical devices for better monitoring of disease progression and patient tracking.

Khan *et al.* [20], the objective was to address significant issues in modern healthcare settings related to complex applicational connectedness, heterogeneity, integrity, privacy protection, security, provenance, and massive volume of everyday media data by developing a novel interoperable technique that resolves three main problems: seamless data integrity, peer-to-peer communication between nodes, and infrastructure security in AI-enabled healthcare environments. The methodology involved integrating blockchain technology for distributed storage data organization, sharing, and exchange with AI-enabled machine learning models, particularly support vector machines, to provide decentralized, secure, economical resource optimization and intelligent network activities and organization, utilizing simulation-based evaluation across three areas: infrastructure security for automated decision-making protection, integrity between smooth data sharing and exchange, and network resource optimization for smooth communication across heterogeneous devices. The findings demonstrated that the proposed novel interoperable architecture achieved unique results with significant improvements showing huge differences of 1.37%, 1.56%, and 1.87% respectively across the three evaluation areas, effectively addressing the complex challenges of end-to-end device interconnectivity, resource organization, communication, networking, and application-related aspects in ICT environments while resolving issues with resource management, scalability, and data processing in distributed consortium networks through the integration of blockchain technology and machine learning models.

Selvamuthu *et al.* [21] investigates how health insurance schemes across diverse Asian populations influence access to secure IoMT-based healthcare services and the extent to which these schemes support cybersecurity investment and infrastructure for vulnerable communities. A mixed-method study combining a policy review of national health insurance programs in India, Indonesia, and the Philippines with

qualitative interviews of 100 patients and 50 healthcare providers. The study reveals that while IoMT adoption is increasing in public and private healthcare facilities, its secure implementation is often constrained by insurance coverage gaps, digital illiteracy, and uneven infrastructure. National health insurance schemes rarely account for cybersecurity costs in IoMT maintenance, leaving patients exposed to risks like data breaches and faulty diagnostics. The authors recommend the inclusion of digital infrastructure and cybersecurity as reimbursable services under public insurance, arguing this would promote equity and reduce care disparities in digital healthcare.

Gopalan *et al.* [22] assesses the feasibility and impact of integrating IoMT-enabled biosensors and blockchain in monitoring food adulteration's effect on public health, particularly in India, where food contamination is a persistent issue. Case analysis of three smart healthcare systems in urban Indian hospitals using biosensor-linked ingestible IoMT devices to track toxin levels in patients, combined with interviews of food safety officials. IoMT devices equipped with smart biosensors detected elevated toxin levels related to food adulteration, triggering early medical interventions and public alerts via blockchain-based health registries. This application of IoMT improves both diagnosis speed and traceability of foodborne illnesses. The study concludes that cross-sector integration of food and health IoT systems can significantly reduce the long-term burden of adulterated food on healthcare systems, but it calls for robust privacy controls to prevent misuse of patient dietary data.

Gopalan *et al.* [23] analyses the legal complexities arising from cybersecurity breaches in IoMT-based telemedicine systems under Indian law, with a focus on liability in medical negligence cases. A doctrinal legal analysis using key statutes such as the Indian Medical Council Act, IT Act, and judgments from Indian courts on telemedicine and data breaches, supported by real-world case studies from Indian hospitals. The study finds that Indian legal frameworks are still evolving to handle liability related to IoMT-based malpractice. Courts have inconsistently applied negligence standards in cases involving data loss or device malfunction. A notable gap is the lack of clear statutory requirements for encryption and cybersecurity standards for IoMT devices in telemedicine consultations. The paper proposes legal reforms to mandate minimum cybersecurity compliance for IoMT vendors and liability protection mechanisms for patients, akin to product liability norms.

Vandana *et al.* [24] explores the synergistic integration of music therapy with IoMT-based mental health monitoring systems, aiming to provide a non-invasive, personalized, and secure treatment modality for psychological well-being. An interdisciplinary experimental study combining wearable EEG-based IoMT sensors with algorithm-driven music therapy sessions personalized by machine learning algorithms. The experiment was conducted on 120 patients diagnosed with mild to moderate depression across two digital mental health clinics. The results showed that real-time monitoring of neural responses through IoMT-enabled wearables combined with responsive music therapy significantly reduced anxiety and depressive symptoms over a 6-week period. Data privacy was maintained using edge computing and anonymized data encryption protocols. The authors advocate for the development of cybersecure IoMT platforms tailored to alternative medicine therapies, highlighting this approach as a low-risk, high-benefit adjunct to traditional mental health treatment.

METHODOS

The research methodology follows an empirical study that explores the cybersecurity threats and vulnerabilities in the Internet of Medical Things (IoMT) ecosystem, with a special focus on public perceptions, trust levels, and awareness regarding connected healthcare devices and their associated security risks. The research aims to assess public understanding of major cybersecurity threats in IoMT devices, identify the most vulnerable components within the IoMT ecosystem, evaluate the perceived frequency and impact of cyberattacks on medical devices, examine factors influencing public trust in connected healthcare devices, and understand public preferences for cybersecurity improvement strategies in healthcare technology. The study is based on a sample size of 206 structured responses collected through a Google Forms-based survey circulated among the general public, using convenient sampling methods to target respondents with varying demographic backgrounds and educational qualifications. The independent variables in this study include demographic factors such as age (18-30, 31-40, 41-50, 51-60, above 60), gender (male, female, transgender), place of residence (urban, semi-urban, rural), and educational qualification (diploma, undergraduate, postgraduate, PhD/MPhil), which serve as categorical variables to analyse how different demographic groups perceive IoMT cybersecurity threats and vulnerabilities. The dependent variables include identification of major cybersecurity threats in IoMT devices (ransomware attacks, unauthorized access, data interception during transmission, software vulnerabilities, lack of encryption), perceived most vulnerable component in the IoMT ecosystem (device hardware, device firmware/software, network communication, cloud storage, mobile applications), frequency perception of cyberattacks on IoMT devices, agreement levels regarding life-threatening potential of cyberattacks, impact rating of data breaches on patient privacy, identification of potential patient harm from hacked devices, factors affecting public trust in connected healthcare devices, preferred approaches for improving IoMT cybersecurity, training necessity perceptions for healthcare professionals, and importance ratings for collaboration between healthcare providers and cybersecurity experts. The survey also measures specific trust factors, cybersecurity improvement preferences, and collaboration importance using Likert scales and rating systems to capture nuanced public opinions. The collected

data will be analysed using statistical tools, including graphical representations, chi-square tests for association analysis, and descriptive statistics to identify key trends, patterns, and correlations between respondents' demographic characteristics and their perceptions of IoMT cybersecurity threats, vulnerabilities, and improvement strategies.

RESULTS

Cross Tabs (Table 1)

Null Hypothesis: There is no association between the respondents' choice of most vulnerable component in Internet of medical Things and their educational qualification.

Alternative Hypothesis

There is an association between the respondents' choice of most vulnerable component in Internet of medical Things and their educational qualification.

Chi-Square Test (Table 2)

The calculated p-value is 0.339. Since the p-value >0.05, the null hypothesis is accepted. So, there is no association between the respondents' choice of most vulnerable component in Internet of medical Things and their educational qualification.

Figure 1 shows that software vulnerabilities are the most significant cybersecurity threat across all age groups, with the 51-60 age group reporting the highest concern (6.8%). Ransomware attacks show notable variation across age groups, with older adults (above 60) showing higher concerns (5.8%) compared to younger groups. Data interception during transmission and unauthorized access show relatively consistent patterns across age groups, with percentages ranging from 3.8% to 4.6%.

Figure 2 shows that cybersecurity threat perception varies significantly by place of residence. Ransomware attacks are most concerning in rural areas (9.7%), while software vulnerabilities show highest concern in rural areas (9.7%). Urban residents show greater concern for unauthorized access (5.8%) compared to rural (5.8%) and semi-urban (6.3%) residents. Data interception during transmission shows relatively consistent concern across all residential categories.

Table 1: Educational qualification × Most vulnerable component (Crosstab)

Educational qualification	Cloud storage	Device firmware/ software	Mobile applications	Network communication	The device hardware	Total
Diploma	8	18	14	13	8	61
PG	11	4	10	11	8	44
PhD/MPhil	10	8	10	13	10	51
UG	11	7	8	10	14	50
Total	40	37	42	47	40	206

Table 2: Chi-Square Tests

Test	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	13.635	12	0.325
Likelihood Ratio	13.420	12	0.339
N of Valid Cases	206		

Note: 0 cells (0.0%) have expected count less than 5. The minimum expected count is 7.90.

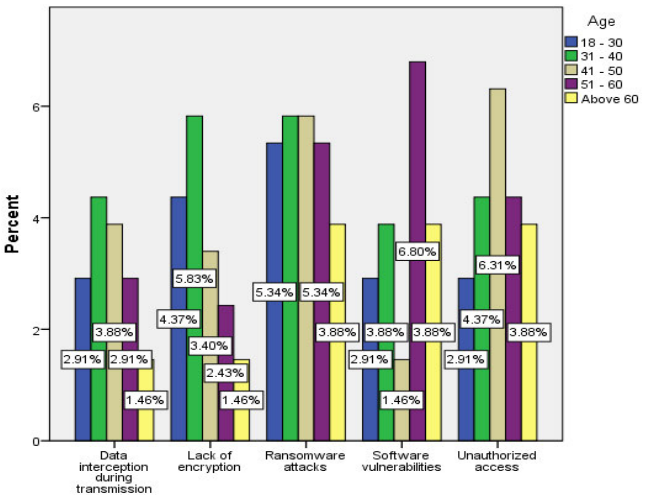

Figure 1: The distribution of major cybersecurity threats across different age groups

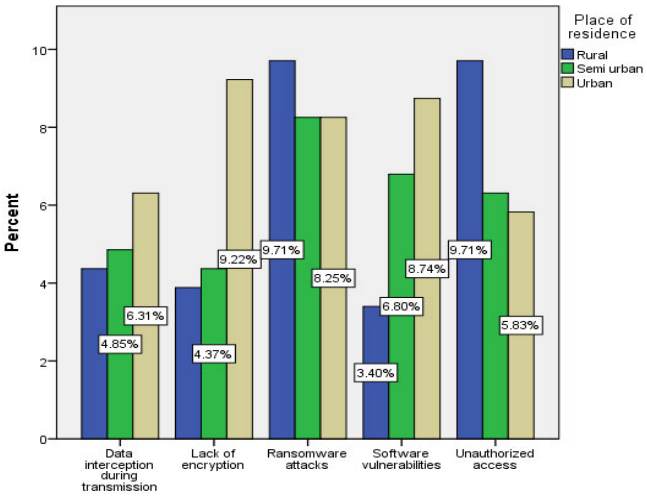

Figure 2: The distribution of major cybersecurity threats across different places of residence

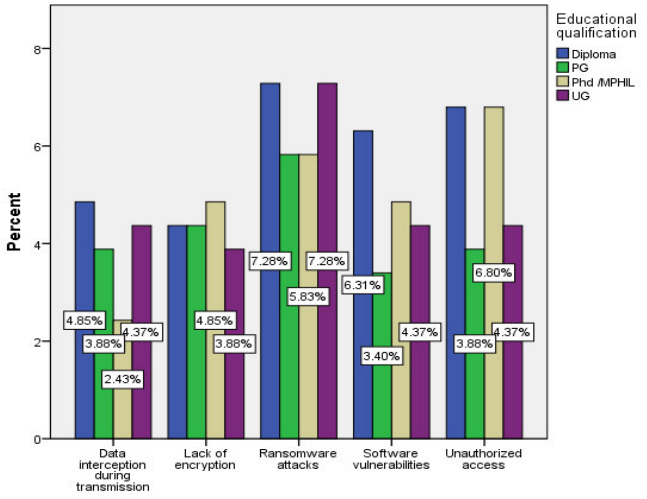

Figure 3: The distribution of major cybersecurity threats across different educational qualifications

Figure 3 shows that educational qualification influences cybersecurity threat perception. Respondents with postgraduate education show highest concern for ransomware attacks (7.3%), while those with undergraduate degrees show greatest concern for software vulnerabilities (6.8%). Lack of encryption concerns are highest among diploma holders (4.9%), while unauthorized access concerns are relatively consistent across educational levels.

Figure 4 shows that cloud storage and device firmware/software are perceived as most vulnerable components across educational qualifications. Respondents with undergraduate degrees show highest concern for device firmware/software (8.7%), while those with postgraduate education show greatest concern for cloud storage (5.5%). Mobile applications and network communication show moderate vulnerability concerns across all educational levels.

Figure 5 shows that vulnerability perceptions vary by residence. Urban residents show highest concern for cloud storage (10.7%), while rural residents show greatest concern for mobile applications (8.2%). Semi-urban residents show balanced concern across all components. Device hardware shows relatively consistent vulnerability ratings across residential categories.

Figure 6 shows that age influences vulnerability perception significantly. The 41-50 age group shows highest concern for device hardware (6.8%), while the 31-40 age group shows greatest concern for cloud storage (5.9%). Mobile applications show relatively consistent vulnerability concerns across age groups, with percentages ranging from 3.9% to 5.5%.

Figure 7 shows that cyberattack frequency varies by age group. The 31-40 age group reports highest frequency of attacks occurring "very frequently" (5.8%), while the 51-60 age group shows highest reports of "never" experiencing attacks (6.3%). Younger adults (18-30) show more balanced distribution across frequency categories.

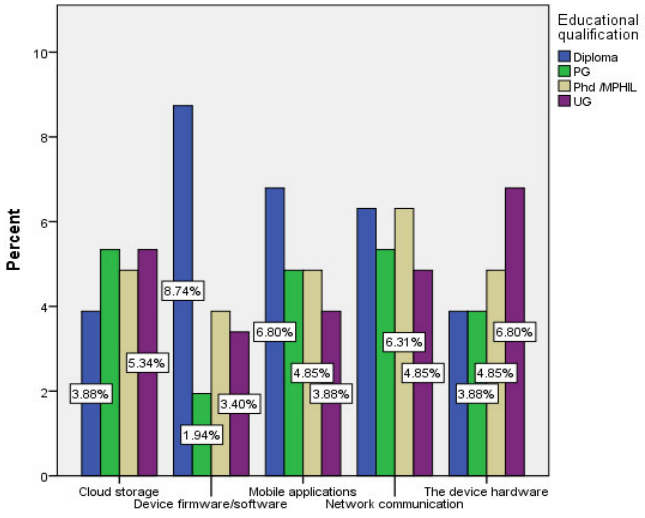

Figure 4: The distribution of most vulnerable components across different educational qualifications

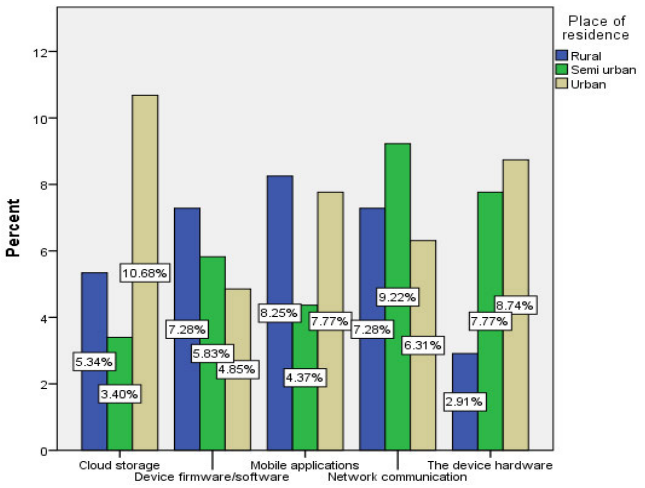

Figure 5: The distribution of most vulnerable components across different places of residence

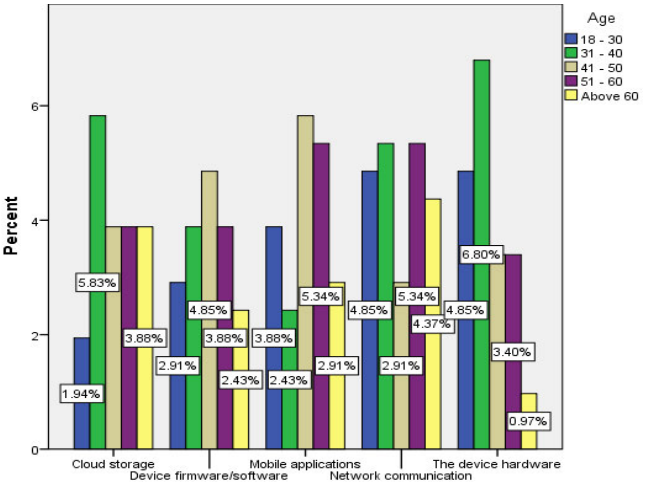

Figure 6: The distribution of most vulnerable components across different age groups

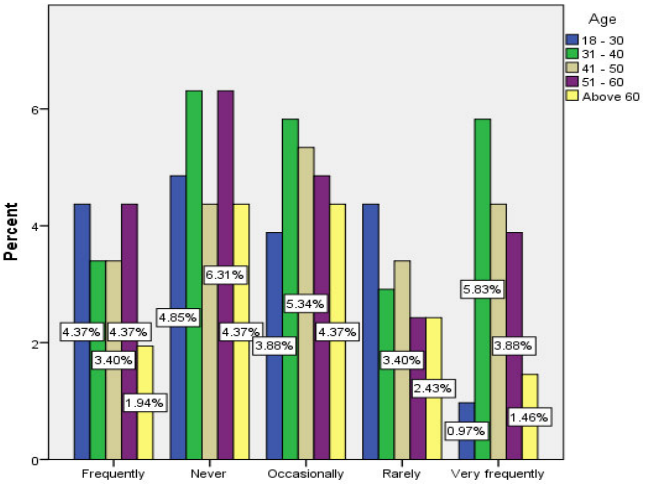

Figure 7: The frequency of cyberattacks across different age groups

Figure 8 shows that attack frequency patterns differ by residence. Urban residents report highest frequency of "never" experiencing attacks (9.2%), while rural residents show more distributed patterns across frequency categories. Semi-urban residents show intermediate patterns between rural and urban responses.

Figure 9 shows that educational qualification affects reported attack frequency. Respondents with postgraduate education report highest frequency of "never" experiencing attacks (9.2%), while those with undergraduate degrees show more varied frequency patterns. Diploma holders show relatively lower frequency of attacks across all categories.

Figure 10 shows that responses to life-threatening situations vary by educational qualification. Respondents with postgraduate education show highest agreement (6.8%) with addressing life-threatening situations, while those with undergraduate degrees show more neutral responses (6.3%). Diploma holders show relatively consistent responses across all agreement levels.

Figure 11 shows that residential location influences responses to life-threatening situations. Urban residents show highest neutral responses (9.7%), while rural residents show more agreement patterns. Semi-urban residents show balanced distribution across response categories.

Figure 12 shows that age affects responses to life-threatening situations. The 31-40 age group shows highest neutral responses (8.3%), while older adults show more agreement patterns. Younger adults show more distributed responses across categories.

Figure 13 shows that patient privacy impact concerns vary by age. The 51-60 age group shows highest concern for severe privacy impact (7.3%), while younger adults show more moderate concern levels. The impact ratings show generally increasing concern with age.

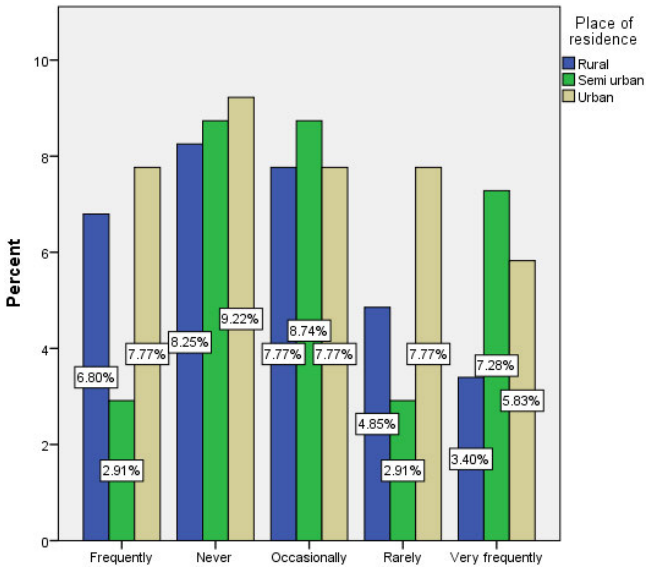

Figure 8: The frequency of cyberattacks across different places of residence

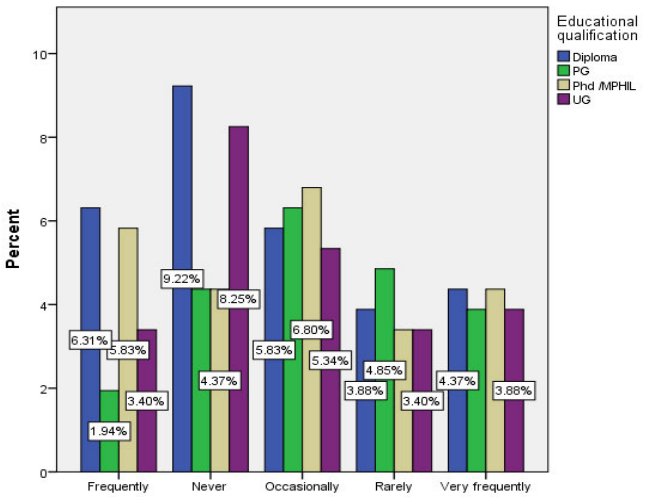

Figure 9: The frequency of cyberattacks across different educational qualifications

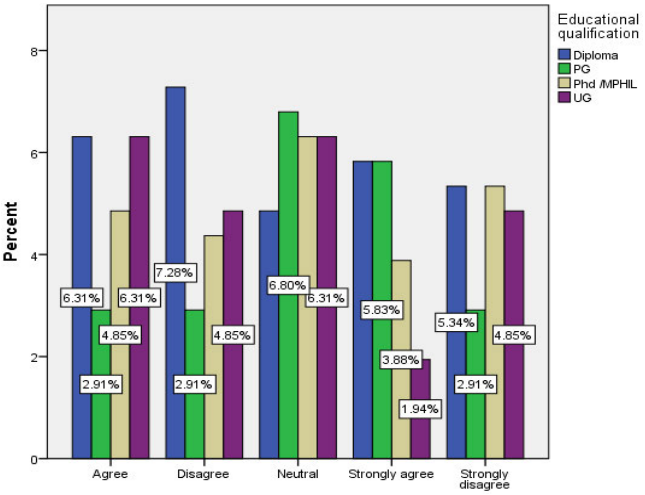

Figure 10: The responses to life-threatening situations across different educational qualifications

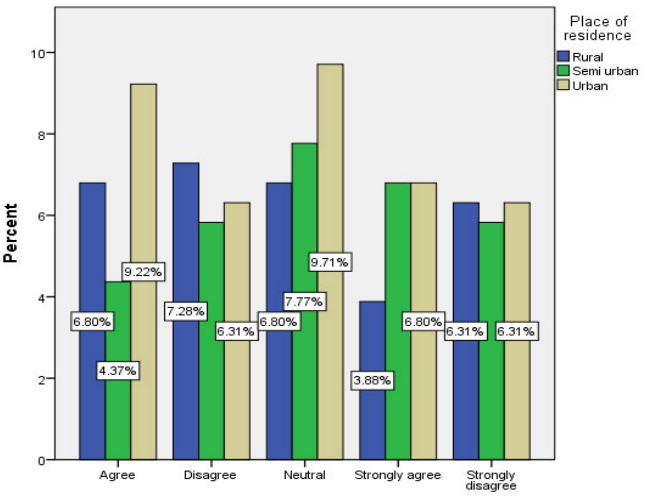

Figure 11: The responses to life-threatening situations across different places of residence

Figure 14 shows that privacy impact concerns differ by residence. Urban residents show highest concern for severe privacy impact (11.0%), while rural residents show more moderate concern levels. Semi-urban residents show intermediate concern patterns.

Figure 15 shows that educational qualification influences privacy impact concerns. Respondents with diploma education show highest concern for severe privacy impact (11.7%), while those with postgraduate education show more distributed concern levels across impact categories.

Figure 16 shows that patient harm types vary by educational qualification. Delay in critical care shows highest concern among respondents with postgraduate education (10.7%), while data theft concerns are highest among diploma holders (7.8%). Psychological distress shows relatively consistent concern across educational levels.

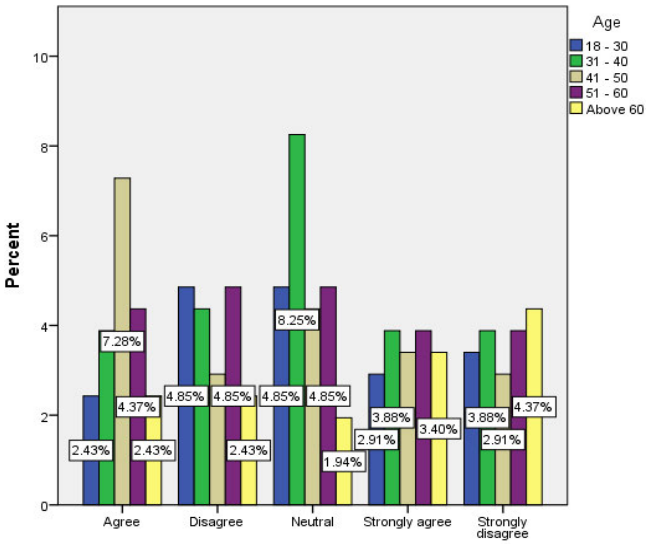

Figure 12: The responses to life-threatening situations across different age groups

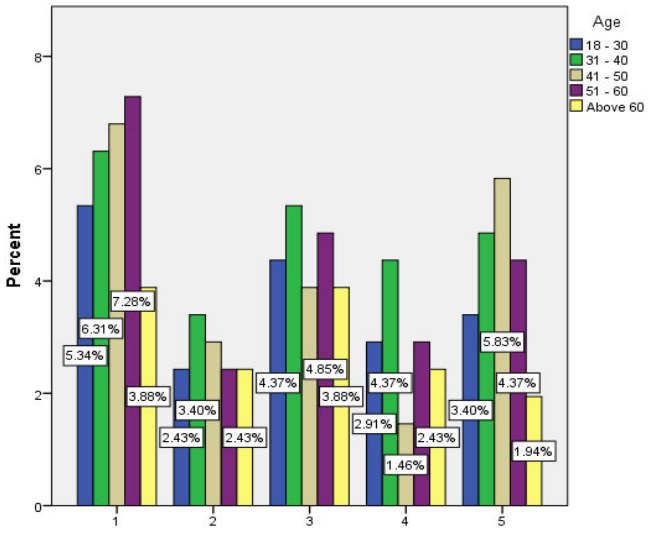

Figure 13: The impact on patient privacy across different age groups

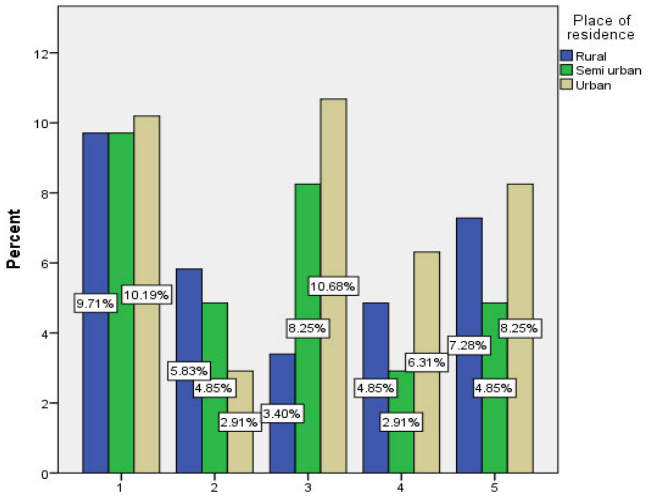

Figure 14: The impact on patient privacy across different places of residence

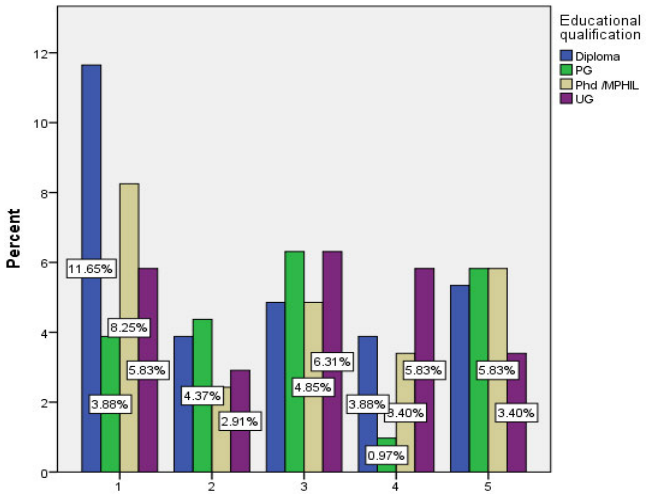

Figure 15: The impact on patient privacy across different educational qualifications

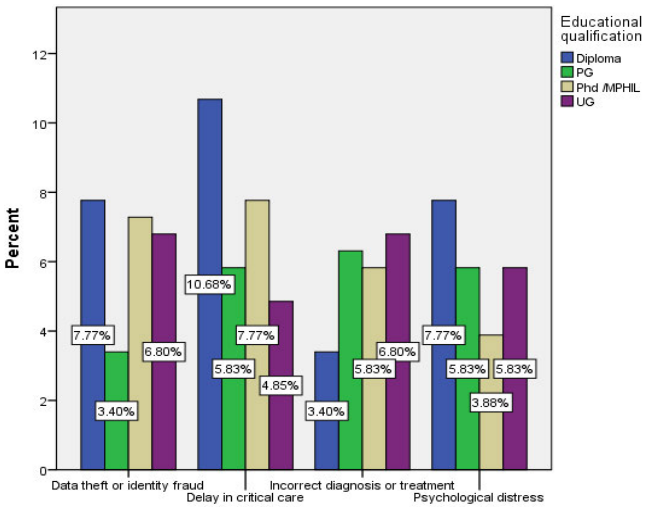

Figure 16: The types of patient harm across different educational qualifications

Figure 17 shows that patient harm concerns differ by residence. Urban residents show highest concern for data theft (11.7%), while rural residents show greatest concern for delays in critical care (11.0%). Semi-urban residents show intermediate concern levels across harm types.

Figure 18 shows that age influences patient harm concerns. The 31-40 age group shows highest concern for delays in critical care (8.3%), while older adults show greater concern for data theft. Psychological distress concerns remain relatively consistent across age groups.

Figure 19 shows that trust factors vary by age. The 51-60 age group shows highest concern for risk of data leaks (6.8%), while younger adults show greater trust in government regulations. Media coverage of cyber incidents shows increasing concern with age.

Figure 20 shows that trust factors differ by residence. Urban residents show highest concern for risk of data leaks (9.2%) and trust in hospital/doctor (9.2%), while rural residents show more balanced trust patterns. Semi-urban residents show intermediate trust levels across factors.

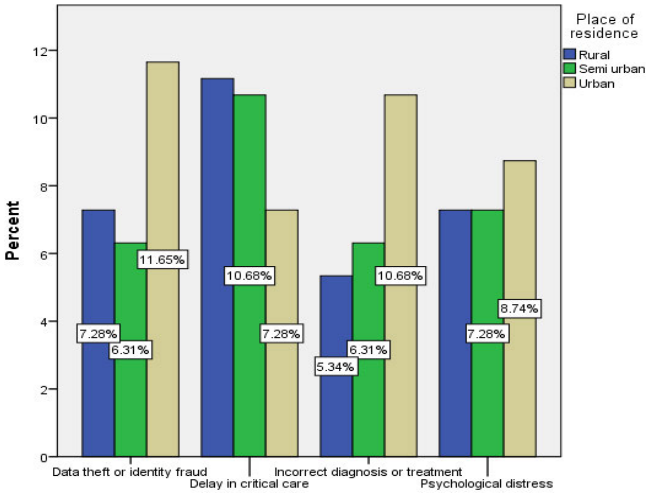

Figure 17: The types of patient harm across different places of residence

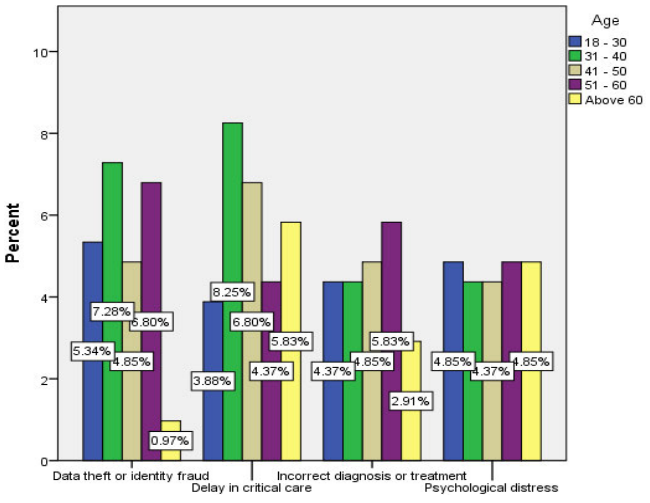

Figure 18: The types of patient harm across different age groups

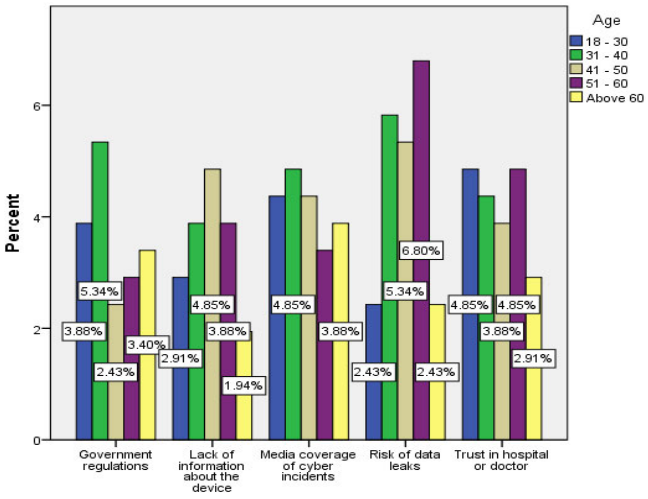

Figure 19: The trust factors across different age groups

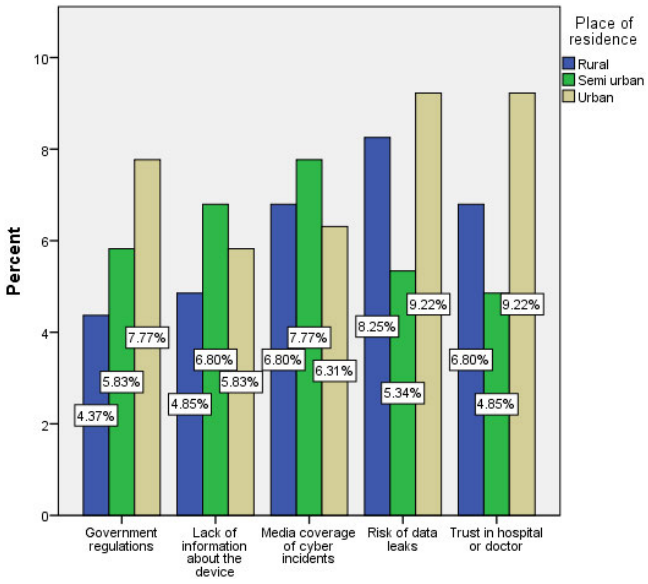

Figure 20: The trust factors across different places of residence

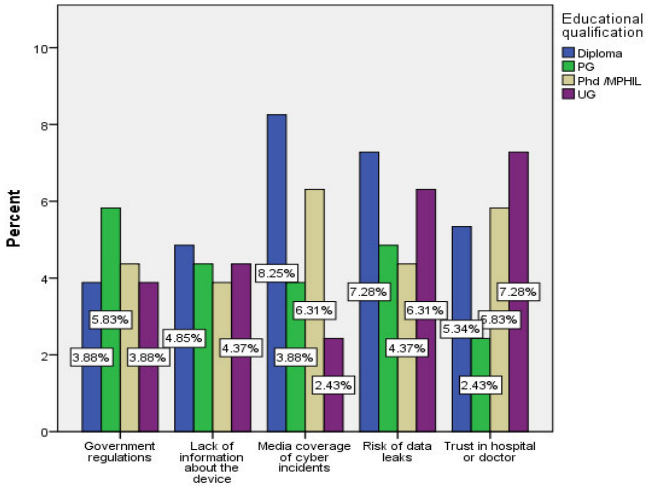

Figure 21: Distribution of trust factors affecting cybersecurity adoption across different educational qualifications (Diploma, PG, PhD/MPhil, UG)

Figure 21 shows that media coverage of cyber incidents emerges as the strongest trust factor across all educational levels, with diploma holders showing the highest concern (8.3%). Trust in hospital or doctor remains consistently moderate across groups (5.3-7.3%), while government regulations show varied impact with postgraduate respondents demonstrating higher trust (5.8%) compared to other groups.

Figure 22 shows that stronger regulatory policies are most favoured by PhD/MPhil holders (7.8%), while increased budget allocation receives highest support from postgraduate respondents (7.1%). Cybersecurity awareness programs show relatively uniform support across educational levels (6.2-6.9%), indicating broad consensus on their importance.

Figure 23 shows that urban residents strongly favour stronger regulatory policies (9.8%), significantly higher than rural (8.7%) and semi-urban (4.5%) populations. Increased budget allocation receives highest support from semi-urban residents (9.2%), while mandatory encryption standards show moderate support across all residence types (5.2-7.3%).

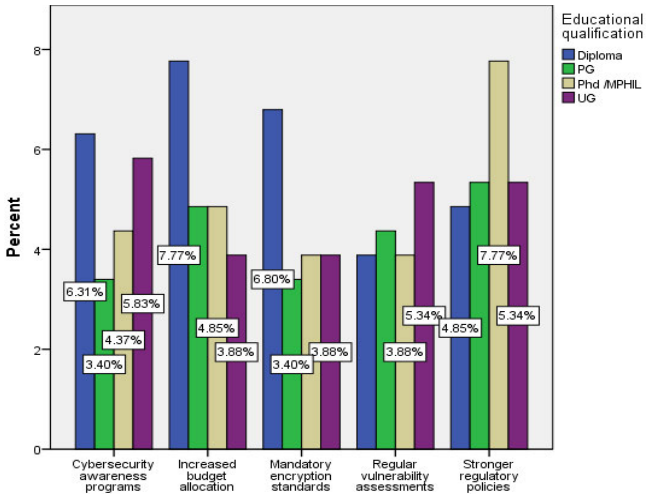

Figure 22: The perceived best cybersecurity improvements categorized by educational qualification levels

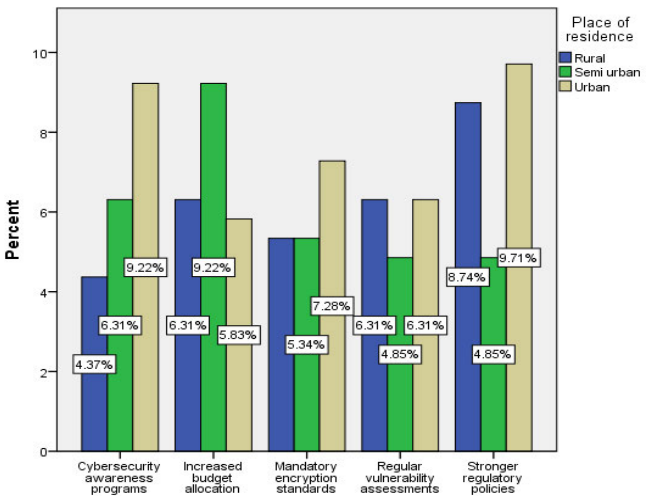

Figure 23: Relationship between place of residence (Rural, Semi-urban, Urban) and preferred cybersecurity improvements

Figure 24 shows that the 31-40 age group demonstrates strongest preference for increased budget allocation (7.2%), while the 51-60 age group favours stronger regulatory policies (7.2%). Cybersecurity awareness programs receive consistent support across age groups (4.4-4.9%), with mandatory encryption standards showing moderate variation by age.

Figure 25 shows that the 31-40 age group exhibits highest agreement for training necessity (7.5%), while the 18-30 age group shows more neutral positions (6.3%). Strong disagreement with training necessity is most pronounced in the 51-60 age group (5.4%), indicating generational differences in training perceptions.

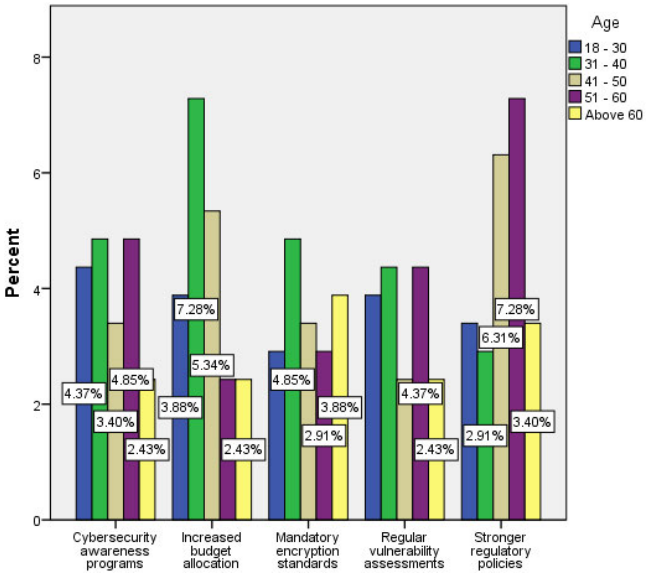

Figure 24: The correlation between age groups and preferred cybersecurity improvement strategies

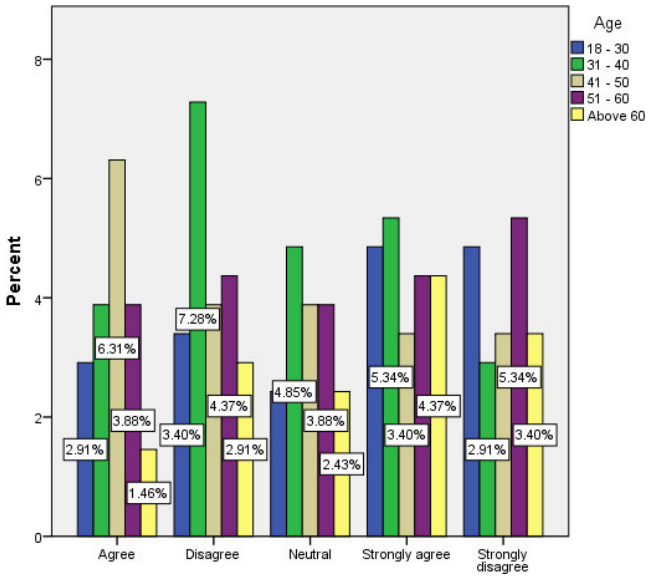

Figure 25: The distribution of training necessity perceptions across different age demographics

Figure 26 shows that urban residents demonstrate highest agreement with training necessity (9.7%), substantially exceeding rural (7.8%) and semi-urban (7.7%) populations. Strong disagreement is most prevalent among rural residents (9.3%), suggesting urban-rural divides in training acceptance.

Figure 27 shows that diploma holders exhibit strongest agreement with training necessity (8.7%), while undergraduate students show more neutral positions (6.4%). PhD/MPhil holders demonstrate highest strong disagreement (6.8%), indicating potential overconfidence in existing knowledge among highly educated respondents.

Figure 28 shows that diploma holders rate collaboration importance highest (11.6% for highest importance), while undergraduate students show more moderate ratings (8.3%). The importance rating decreases progressively from rating 1 to 5 across all educational levels, with postgraduate respondents showing consistent moderate importance ratings.

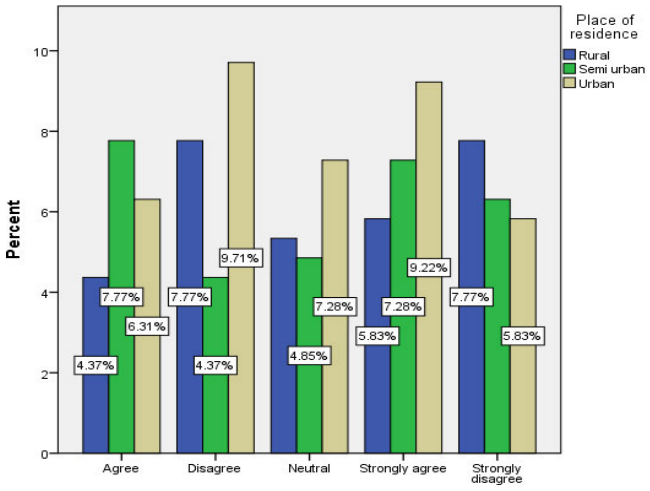

Figure 26: The relationship between place of residence and perceived training necessity for cybersecurity

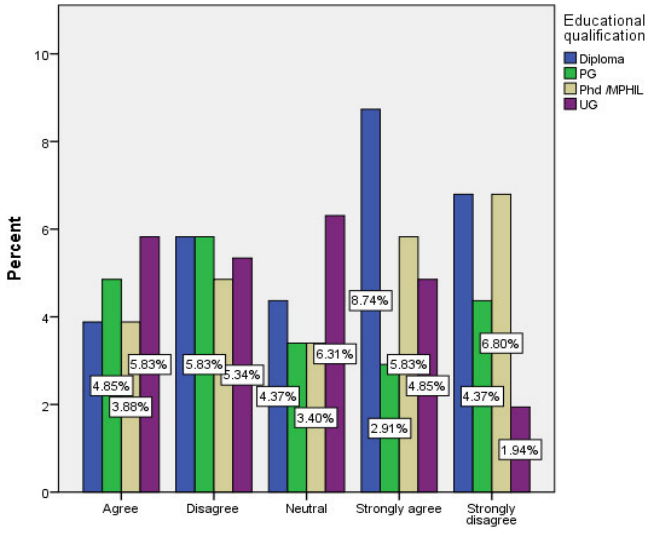

Figure 27: The association between educational qualification and training necessity perceptions

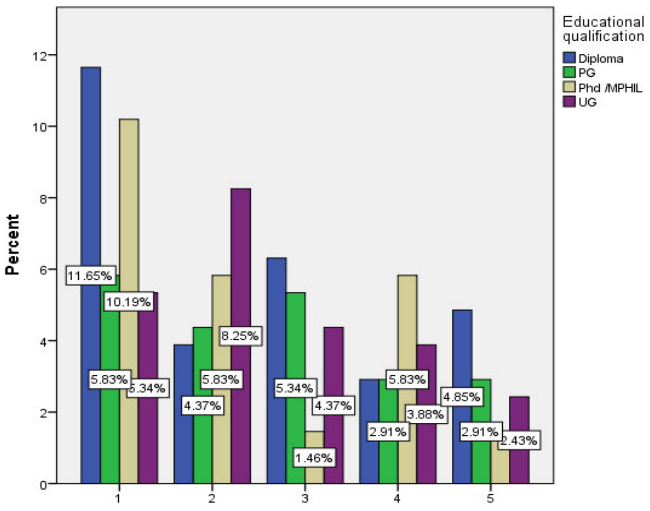

Figure 28: The importance of collaboration in cybersecurity across different educational backgrounds

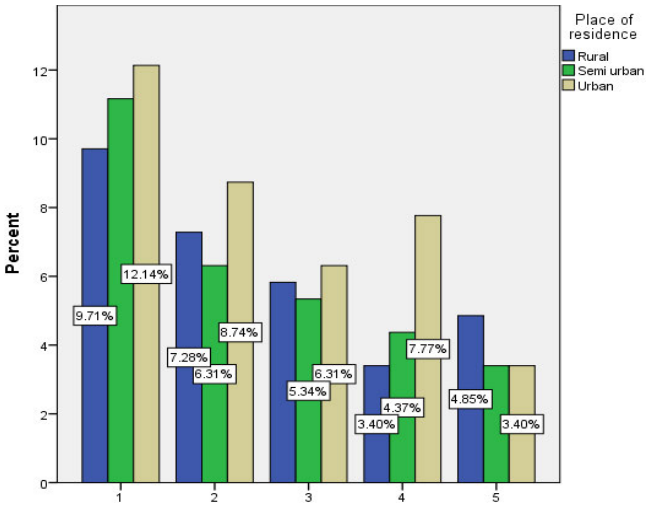

Figure 29: The relationship between place of residence and collaboration importance ratings

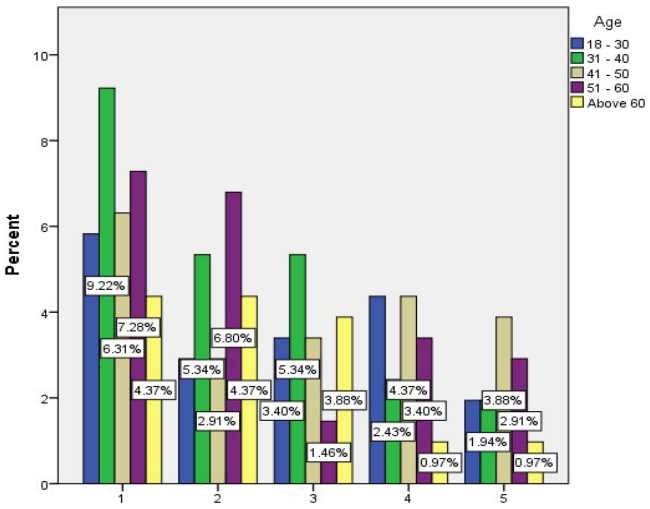

Figure 30: The correlation between age groups and perceived collaboration importance in cybersecurity

Figure 29 shows that urban residents assign highest importance to collaboration (12.2% for top rating), followed by semi-urban (11.1%) and rural (9.7%) populations. The importance perception decreases consistently across rating levels, with rural residents showing lowest importance ratings for collaboration.

Figure 30 shows that the 31-40 age group attributes highest importance to collaboration (9.2% for top rating), while older age groups (above 60) show diminishing importance ratings (4.3%). The 18-30 age group demonstrates moderate importance perception (5.8%), with importance ratings generally decreasing with advancing age.

DISCUSSION

The statistical analysis reveals a p-value of 0.339 for the association between respondents' identification of the most vulnerable component in the Internet of Medical Things (IoMT) and their educational qualification (Table 2), which is substantially greater than the conventional significance threshold of 0.05, leading to acceptance of the null hypothesis and indicating no statistically significant association between educational qualification and perceived vulnerability in IoMT components. This finding suggests that educational background does not significantly influence how individuals assess cybersecurity risks in medical technology environments, indicating a convergence of risk perception across educational levels that may reflect widespread media coverage of healthcare cybersecurity incidents creating a common baseline of awareness that transcends educational boundaries, the intuitive nature of certain IoMT vulnerabilities making them apparent to individuals regardless of formal educational background, and the life-critical nature of medical devices making security concerns more tangible and immediate for all users. The absence of educational differentiation suggests that certain IoMT vulnerabilities are universally recognized across educational levels, possibly because these vulnerabilities often manifest in ways visible to end users and because practical experience with medical technology may be more influential than formal education in identifying vulnerabilities, as users develop intuitive understanding of system weaknesses through direct interaction. This finding has important implications for cybersecurity training and policy development, suggesting that training programs should be designed with the assumption that vulnerability recognition capabilities are relatively uniform across educational levels, allowing for more standardized approaches to cybersecurity education rather than complex, education-level-specific programs, while policy developers should recognize that cybersecurity awareness initiatives in healthcare settings can target broad audiences without significant educational differentiation. The result supports the development of universal cybersecurity training programs while emphasizing the importance of practical experience and specialized expertise in healthcare technology security, suggesting that healthcare organizations can implement inclusive cybersecurity awareness programs that leverage universal vulnerability recognition capabilities while providing specialized training for technical implementation and advanced threat assessment, making inclusive stakeholder engagement in healthcare cybersecurity planning more feasible than previously thought since vulnerability perception appears consistent across educational demographics.

Figure 1 demonstrates that software vulnerabilities represent the most universally recognized cybersecurity threat across all age demographics, suggesting a widespread awareness of system weaknesses that transcends generational boundaries. This finding indicates that regardless of technological familiarity or digital nativity, individuals across all age groups recognize the inherent risks posed by software flaws and security gaps. The higher concern levels among older adults (51-60 age group) for ransomware attacks may reflect their increased exposure to targeted cybercriminal campaigns that specifically exploit this demographic's potentially limited cybersecurity knowledge and higher financial assets. This pattern could also indicate the effectiveness of media campaigns and educational initiatives that have highlighted ransomware threats to older populations. The consistent patterns in data interception concerns across age groups indicate a fundamental understanding of transmission security risks that suggests successful public awareness campaigns about the vulnerabilities inherent in data transmission processes. This universal concern may also reflect the increasing prevalence of public Wi-Fi usage and the growing awareness of man-in-the-middle attacks across all age demographics.

Figure 2 reveals significant geographical disparities in cybersecurity threat perception, with rural residents showing disproportionately high concern for ransomware attacks compared to their urban and semi-urban counterparts. This pattern may reflect the limited cybersecurity infrastructure available in rural areas, where residents may rely on outdated systems, have limited access to professional IT support, and face challenges in implementing comprehensive security measures. The higher vulnerability in rural areas could also stem from the prevalence of older computing systems and potentially less frequent software updates due to limited internet connectivity or technical support. Urban residents' higher concern for unauthorized access aligns with their likely greater exposure to diverse cyber threats in metropolitan environments, where the concentration of digital services, public Wi-Fi networks, and diverse user populations creates multiple attack vectors. The semi-urban residents' intermediate concern levels suggest a transitional security posture that reflects their position between rural vulnerability and urban security awareness, potentially indicating varying levels of cybersecurity infrastructure development in these emerging urban areas.

Figure 3 indicates that educational background significantly shapes cybersecurity threat assessment, with postgraduate-educated individuals showing heightened awareness of ransomware complexity, potentially due to their professional exposure to sophisticated cyber threats or their

enhanced technical understanding of attack mechanisms. This demographic's higher concern levels may reflect their professional responsibilities in managing sensitive information systems or their exposure to advanced threat intelligence through their work environments. The undergraduate-educated respondents' focus on software vulnerabilities suggests a practical understanding of system weaknesses that may stem from their academic exposure to computer science concepts or their professional experience with software systems. The consistent concern for unauthorized access across educational levels suggests this threat is universally recognized regardless of technical expertise, indicating that basic security awareness about access control has penetrated across all educational demographics. The diploma holders' specific concerns about encryption gaps may reflect their hands-on technical experience in fields where encryption is a daily consideration, such as healthcare informatics or technical support roles.

Figure 4 shows that perceived vulnerability of technological components varies significantly with educational qualification, with undergraduate-educated respondents showing particular concern for device firmware/software vulnerabilities, possibly reflecting their practical experience with system updates, patches, and the consequences of software failures in their professional or academic environments. This demographic's awareness may stem from their direct exposure to software development cycles, beta testing, or IT support roles where firmware vulnerabilities are frequently encountered. The balanced concern for cloud storage among postgraduate-educated individuals may indicate their sophisticated understanding of distributed computing risks, including data sovereignty issues, third-party security dependencies, and the complex threat landscape associated with cloud service providers. Their professional exposure to enterprise-level cloud deployments may provide them with insights into the multifaceted security challenges inherent in cloud computing environments. The diploma holders' moderate but consistent concerns across all components suggest a practical, hands-on understanding of technology vulnerabilities that reflects their technical training and direct experience with system maintenance and troubleshooting.

Figure 5 demonstrates geographical variations in vulnerability perception, with urban residents showing significantly higher concern for cloud storage vulnerabilities, reflecting their greater adoption of cloud-based services for both personal and professional use. Urban environments typically feature more advanced digital infrastructure, higher internet penetration rates, and greater integration of cloud services into daily life, leading to increased awareness of associated security risks. The rural residents' focus on mobile applications may indicate their primary reliance on mobile technology for accessing digital services, possibly due to limited broadband infrastructure or the convenience of mobile-first service delivery in areas with sparse traditional computing infrastructure. This pattern suggests that rural populations may be particularly vulnerable to mobile-specific threats due to their concentrated reliance on these platforms. Semi-urban residents' intermediate concern levels reflect their transitional position between rural mobile-centricity and urban cloud adoption, potentially indicating a diversified technology usage pattern that encompasses both traditional and emerging digital service delivery methods.

Figure 6 reveals age-related patterns in vulnerability assessment, with middle-aged adults (41-50) showing highest concern for device hardware vulnerabilities, possibly reflecting their professional experience with system failures, hardware lifecycle management, and the economic impact of hardware-related security breaches. This demographic's concerns may stem from their role in organizational decision-making regarding technology investments and their direct experience with the consequences of hardware security failures. The consistent mobile application concerns across age groups suggest universal adoption and awareness of mobile security risks, indicating that mobile security threats have achieved widespread recognition regardless of generational differences in technology adoption. Younger adults' relatively lower concern for cloud storage may reflect their normalized relationship with cloud services, having grown up with these technologies and potentially developing a higher risk tolerance through familiarity. Older adults' elevated concerns across multiple categories may indicate a more cautious approach to technology adoption and a heightened awareness of potential security implications.

Figure 7 indicates that cyberattack frequency reporting varies significantly by age, with the 31-40 age group's higher reporting of frequent attacks possibly reflecting their active digital engagement across multiple platforms, professional exposure to cyber threats, and their position as primary targets for cybercriminals who recognize this demographic's combination of digital sophistication and financial assets. This group's higher attack frequency may also indicate better threat detection capabilities and incident recognition, leading to more accurate reporting of security events. The 51-60 age group's higher "never" responses may indicate either more effective security practices developed through experience, more conservative digital behaviour that reduces attack surface, or alternatively, underreporting due to unrecognized attacks or less sophisticated threat detection capabilities. The younger adults' distributed response patterns may reflect their experimental approach to technology adoption, potentially exposing them to varied threat types while also demonstrating resilience and adaptability in threat response.

Figure 8 shows that residential location significantly influences attack frequency perception, with urban residents' higher "never" responses potentially indicating access to better cybersecurity infrastructure, professional IT support services, and more sophisticated security tools that effectively prevent or mitigate attacks. Alternatively, this pattern might reflect less recognition of subtle attacks due to the complexity of urban digital environments where minor security incidents may go unnoticed among the high volume of digital interactions. The distributed patterns among rural

residents may reflect varied cybersecurity preparedness levels, with some individuals implementing effective security measures while others remain vulnerable due to limited access to cybersecurity resources, training, or support services. Semi-urban residents' intermediate patterns suggest a transitional security posture that reflects their evolving digital infrastructure and varying levels of cybersecurity awareness and implementation.

Figure 9 demonstrates that educational qualification significantly affects attack frequency reporting, with postgraduate-educated individuals' higher "never" responses possibly reflecting their access to better cybersecurity practices, professional-grade security measures, or organizational security protocols that effectively prevent attacks. This demographic's lower attack frequency may also indicate their more cautious approach to digital interactions, informed by their understanding of cyber threat landscapes and risk management principles. The varied patterns among undergraduate-educated respondents may indicate diverse exposure levels based on their specific fields of study, professional environments, and personal digital habits. Diploma holders' relatively moderate frequency patterns may reflect their practical, hands-on approach to cybersecurity that balances accessibility with security considerations, potentially leading to a more realistic assessment of their actual attack experiences.

Figure 10 reveals that educational background significantly influences responses to life-threatening cybersecurity situations, with postgraduate-educated individuals showing higher agreement levels, possibly reflecting their professional understanding of critical system dependencies, their exposure to risk management frameworks, and their comprehension of the potential cascading effects of cybersecurity failures in critical infrastructure. This demographic's higher agreement may also indicate their professional responsibility for risk assessment and their familiarity with business continuity planning that emphasizes the life-critical nature of certain cybersecurity threats. The neutral responses among various groups may indicate uncertainty about appropriate responses to such scenarios, suggesting a need for enhanced public education about the potential life-threatening implications of cybersecurity failures. The varied response patterns may also reflect different levels of exposure to critical infrastructure systems and varying degrees of understanding about the interconnected nature of digital and physical safety systems.

Figure 11 shows that residential location affects life-threatening situation responses, with urban residents' higher neutral responses potentially indicating either better preparedness through access to multiple redundant systems, or conversely, greater uncertainty about cyber-physical security risks due to the complexity of urban infrastructure systems. The urban neutral stance may reflect a more sophisticated understanding of the multi-layered security systems that protect critical infrastructure, leading to a more nuanced view of threat severity. The agreement patterns among rural residents may reflect community-based response approaches, greater reliance on local support systems, and potentially higher awareness of their vulnerability to system failures due to limited redundancy in rural infrastructure. Semi-urban residents' intermediate responses suggest a transitional understanding that combines urban system complexity awareness with rural community resilience approaches.

Figure 12 indicates that age significantly influences life-threatening situation assessment, with middle-aged adults showing more neutral responses, possibly reflecting their balanced risk assessment experience gained through professional exposure to various crisis scenarios and their understanding of both system vulnerabilities and resilience mechanisms. This demographic's measured response may indicate their role in organizational crisis management and their realistic assessment of both threats and protective measures. The agreement patterns among older adults may indicate heightened awareness of vulnerability in critical systems, possibly stemming from their lived experience with system failures, their increased dependence on healthcare and other critical services, and their understanding of the potential consequences of system disruptions. Younger adults' varied responses may reflect their experimental approach to risk assessment and their developing understanding of cyber-physical security implications.

Figure 13 demonstrates that patient privacy impact concerns increase substantially with age, with the 51-60 age group showing highest concern levels, possibly reflecting their accumulated experience with privacy violations, their professional exposure to healthcare systems, and their understanding of the long-term consequences of privacy breaches. This demographic's heightened concern may also stem from their increased healthcare utilization and their awareness of the sensitive nature of medical information and its potential for misuse. The moderate concern levels among younger adults may indicate normalized attitudes toward data sharing, reflecting their generation's comfort with digital information exchange and potentially different privacy expectations shaped by their lifelong exposure to social media and digital services. The progressive increase in concern with age suggests that privacy awareness develops through experience and that older adults may have a more comprehensive understanding of the potential implications of privacy violations.

Figure 14 shows that residential location significantly influences privacy impact assessment, with urban residents showing highest concern levels, possibly reflecting their greater exposure to privacy breaches, more sophisticated understanding of healthcare system complexity, and higher awareness of the interconnected nature of digital health records across multiple providers and systems. Urban residents' concerns may also reflect their exposure to media coverage of privacy breaches and their understanding of the potential scale and impact of such incidents in complex healthcare ecosystems. The moderate rural concerns may indicate either better privacy protection through smaller, more isolated healthcare systems, or alternatively, limited awareness

of potential impacts due to less exposure to privacy breach incidents and simpler healthcare delivery systems. Semi-urban residents' intermediate concern levels suggest a transitional privacy awareness that reflects their exposure to both simple and complex healthcare delivery models.

Figure 15 reveals that educational qualification affects privacy impact assessment in unexpected ways, with diploma-educated individuals showing surprisingly high concern levels, possibly reflecting their direct healthcare work experience, their hands-on exposure to healthcare data systems, and their practical understanding of how privacy breaches can impact patient care and trust. This demographic's elevated concern may stem from their professional responsibility for maintaining patient confidentiality and their direct observation of the consequences of privacy violations in healthcare settings. The distributed patterns among postgraduate-educated respondents may indicate their nuanced understanding of privacy implications, reflecting their exposure to privacy frameworks, regulatory requirements, and risk management approaches that provide them with a more complex view of privacy impacts. The varied responses across educational levels suggest that privacy awareness develops through different pathways, with practical experience potentially being as important as formal education in shaping privacy concern levels.

Figure 16 demonstrates that patient harm type assessment varies significantly by educational qualification, with postgraduate-educated individuals showing highest concern for care delays, possibly reflecting their comprehensive understanding of healthcare system dependencies, their awareness of clinical workflow requirements, and their professional exposure to the critical timing requirements in healthcare delivery. This demographic's focus on care delays may indicate their understanding of how cybersecurity incidents can cascade through healthcare systems, affecting multiple patients and care processes. The data theft concerns among diploma holders may indicate their direct exposure to healthcare data vulnerabilities through their hands-on work with patient information systems, their understanding of the practical implications of data breaches, and their professional responsibility for data protection. The consistent psychological distress concerns across educational levels suggest universal recognition of the mental health impacts of cybersecurity incidents, indicating that all healthcare stakeholders understand the emotional and psychological consequences of security breaches.

Figure 17 shows that residential location influences patient harm assessment, with urban residents showing highest data theft concerns, possibly reflecting their greater exposure to healthcare data breaches, their understanding of the complex data sharing arrangements in urban healthcare systems, and their awareness of the potential for large-scale data compromises in metropolitan healthcare networks. The rural residents' concern for care delays may indicate their direct experience with healthcare access challenges, their understanding of the limited redundancy in rural healthcare systems, and their awareness of how cybersecurity incidents can disproportionately impact communities with limited healthcare resources. Semi-urban residents' intermediate concerns suggest a transitional understanding that combines urban data complexity awareness with rural access vulnerability concerns, potentially reflecting their exposure to both centralized and distributed healthcare delivery models.

Figure 18 indicates that age affects patient harm assessment, with middle-aged adults showing highest concern for care delays, possibly reflecting their active healthcare engagement, their caregiving responsibilities for both children and aging parents, and their professional understanding of healthcare system dependencies. This demographic's concern for care delays may stem from their direct experience with healthcare scheduling complexities and their understanding of how system disruptions can affect critical care timing. The consistent psychological distress concerns across age groups suggest universal recognition of cybersecurity's mental health impacts, indicating that all age demographics understand the emotional consequences of security breaches and the anxiety associated with healthcare system vulnerabilities. The varied patterns across harm types suggest that different age groups prioritize different aspects of healthcare security based on their specific experiences and vulnerabilities.

Figure 19 reveals that trust factors vary significantly by age, with older adults showing highest concern for data leaks, possibly reflecting their accumulated experience with privacy violations, their understanding of the long-term consequences of data breaches, and their heightened awareness of their vulnerability to identity theft and financial fraud. This demographic's concern may also stem from their limited ability to recover from the consequences of data breaches and their understanding of how personal information can be exploited. The younger adults' greater trust in government regulations may indicate generational differences in institutional confidence, reflecting their exposure to evolving regulatory frameworks and their belief in the effectiveness of policy solutions to cybersecurity challenges. The varied trust patterns across age groups suggest that trust development is influenced by generational experiences, with older adults potentially having more skeptical views based on their historical exposure to institutional failures and privacy violations.

Figure 20 demonstrates that residential location affects trust factor assessment, with urban residents showing highest concern for data leaks and institutional trust, possibly reflecting their greater exposure to both cyber threats and healthcare system complexity, their understanding of the interconnected nature of urban digital systems, and their awareness of the potential scale of data breaches in metropolitan environments. The urban residents' simultaneous high concern for data leaks and high trust in healthcare providers may indicate a nuanced understanding that recognizes both systemic vulnerabilities and the competence of individual healthcare professionals. The balanced rural trust

patterns may indicate community-based confidence in local healthcare providers, reflecting the personal relationships and direct accountability that characterize rural healthcare delivery, potentially leading to higher trust levels despite awareness of systemic vulnerabilities.

Figure 21 shows that media coverage significantly influences cybersecurity trust perceptions across educational levels, suggesting that information dissemination strategies should focus on responsible reporting of cyber incidents. The high impact of media coverage across all educational groups indicates that cybersecurity awareness is heavily shaped by public discourse and news reporting patterns. This finding has important implications for cybersecurity communication strategies, as sensationalized reporting may inadvertently increase anxiety while failing to promote constructive security behaviours. The moderate trust in healthcare institutions indicates potential for sector-specific cybersecurity initiatives, particularly given the sensitive nature of medical data and the increasing digitization of healthcare systems. However, the varied responses to government regulations suggest need for targeted policy communication approaches that address educational differences in regulatory perception. Higher education levels may require more detailed technical explanations of regulatory frameworks, while lower education levels may benefit from simplified, practical guidance on compliance requirements. The relatively consistent trust levels across educational groups for data leak risks and hospital/doctor trust suggests that certain cybersecurity concerns transcend educational boundaries, indicating opportunities for universal messaging strategies.

Figure 22 shows clear educational differences in cybersecurity improvement preferences, with higher education levels favoring regulatory approaches while practical measures like budget allocation receive broader support. This pattern suggests that cybersecurity strategies should incorporate both policy-driven and resource-based improvements to address diverse stakeholder expectations. The preference for regulatory solutions among PhD/MPhil holders likely reflects their familiarity with institutional frameworks and policy implementation processes, while the broad support for budget allocation across all educational levels indicates recognition of resource constraints in cybersecurity implementation. The consistent support for cybersecurity awareness programs across educational groups suggests that knowledge dissemination remains a universal priority, regardless of formal education levels. However, the content and delivery methods of these programs may need to be tailored to different educational backgrounds. The moderate support for mandatory encryption standards across all groups indicates technical awareness but also suggests potential concerns about implementation complexity and costs. These findings imply that cybersecurity improvement strategies should be multi-faceted, combining regulatory frameworks with resource allocation and educational initiatives to address the diverse needs and preferences of different stakeholder groups.

Figure 23 shows significant urban-rural disparities in cybersecurity improvement preferences, with urban populations favoring regulatory solutions while semi-urban areas prioritize resource allocation. These findings indicate the need for location-specific cybersecurity strategies that account for different infrastructure and regulatory environments. Urban areas' preference for stronger regulatory policies likely reflects their exposure to more complex cybersecurity threats and greater institutional capacity for policy implementation. The sophisticated digital infrastructure in urban areas may make regulatory compliance more feasible, while rural areas may face greater challenges in implementing complex regulatory requirements. Semi-urban areas' preference for increased budget allocation suggests recognition of resource gaps that hinder cybersecurity implementation. This may reflect a transitional status where digital adoption is increasing but supportive infrastructure remains limited. The moderate support for mandatory encryption standards across all residence types indicates technical awareness but also suggests potential concerns about implementation complexity in areas with limited technical expertise. Rural areas' lower support for various cybersecurity improvements may reflect limited exposure to cyber threats or skepticism about the relevance of sophisticated cybersecurity measures in their context. These findings suggest that cybersecurity policies should be geographically differentiated, with urban areas receiving more regulatory focus while rural and semi-urban areas benefit from targeted resource allocation and capacity building programs.

Figure 24 shows age-related variations in cybersecurity improvement preferences, with middle-aged groups favoring resource-intensive solutions while older groups prefer regulatory approaches. This suggests that cybersecurity policies should incorporate generational perspectives and tailor implementation strategies accordingly. The 31-40 age group's preference for increased budget allocation likely reflects their active participation in digital systems and direct experience with cybersecurity challenges in professional contexts. This demographic may have greater awareness of the resource requirements for effective cybersecurity implementation. The 51-60 age group's preference for stronger regulatory policies may reflect their preference for institutional solutions and formal frameworks for addressing complex problems. This generation may have greater trust in governmental and regulatory approaches to problem-solving. The consistent support for cybersecurity awareness programs across age groups suggests universal recognition of the importance of education in cybersecurity, though the preferred delivery methods and content may vary by age. Younger groups may prefer digital and interactive training methods, while older groups may favor traditional educational approaches. The moderate variation in support for mandatory encryption standards across age groups indicates technical awareness but also suggests potential concerns about implementation complexity among older demographics. These findings imply that cybersecurity

strategies should be age-sensitive, with resource allocation targeting active digital users while regulatory frameworks appeal to those preferring institutional solutions.

Figure 25 shows generational differences in training necessity perceptions, with younger and middle-aged groups more receptive to training programs while older groups show resistance. This indicates need for age-appropriate training methodologies and addressing potential barriers to participation among senior demographics. The 31-40 age group's highest agreement with training necessity likely reflects their peak professional engagement with digital systems and recognition of rapidly evolving cybersecurity threats. This demographic may experience the most direct impact of cybersecurity challenges in their work environments. The 18-30 age group's more neutral position may reflect confidence in their digital native status and informal learning approaches to cybersecurity. However, this confidence may be misplaced, as technical familiarity does not necessarily translate to security awareness. The 51-60 age group's strong disagreement with training necessity may reflect several factors: perceived irrelevance of cybersecurity training to their digital usage patterns, scepticism about the effectiveness of formal training programs, or overconfidence in existing knowledge. This resistance represents a significant challenge for cybersecurity capacity building, as older demographics may be particularly vulnerable to social engineering attacks while being least likely to participate in protective training programs. The findings suggest that training programs should be differentiated by age, with younger groups receiving advanced technical training while older groups receive basic awareness and practical protective measures training.

Figure 26 shows substantial urban-rural divides in training acceptance, with urban populations more receptive to cybersecurity training initiatives. This suggests that rural cybersecurity capacity building requires different approaches, potentially including community-based programs and addressing infrastructure limitations. Urban residents' high agreement with training necessity likely reflects their greater exposure to cybersecurity threats and more sophisticated digital environments. Urban areas typically have better access to training resources and more developed educational infrastructure. The strong disagreement among rural residents may reflect several factors: limited exposure to cyber threats, scepticism about the relevance of cybersecurity training to their digital usage patterns, or practical barriers to accessing training programs. Rural areas may also have cultural preferences for informal learning and community-based knowledge sharing rather than formal training programs. The semi-urban population's moderate position suggests a transitional status where digital adoption is increasing but training infrastructure remains limited. These findings indicate that rural cybersecurity training programs should be adapted to local contexts, potentially incorporating community leaders and trusted local institutions. Mobile training units, online programs adapted to limited bandwidth, and integration with existing community programs may be more effective than traditional classroom-based approaches.

Figure 27 shows educational paradoxes in training necessity perceptions, with highly educated individuals showing greater resistance to training programs. This suggests that training programs should be differentiated based on existing knowledge levels and address potential overconfidence among educated populations. The diploma holders' strongest agreement with training necessity may reflect their practical orientation and recognition of knowledge gaps in rapidly evolving cybersecurity landscapes. This group may have sufficient technical background to understand cybersecurity complexity while maintaining humility about their expertise. The undergraduate students' neutral position may reflect uncertainty about their cybersecurity knowledge levels and the value of formal training. The PhD/MPhil holders' highest strong disagreement represents a significant challenge, as this group may have the greatest influence on organizational cybersecurity policies while being least receptive to training. This resistance may stem from overconfidence in existing knowledge, time constraints, or belief that their advanced education provides sufficient background for cybersecurity understanding. However, cybersecurity threats evolve rapidly and require continuous learning regardless of educational background. The findings suggest that training programs for highly educated populations should emphasize advanced topics, peer learning, and recognition of existing expertise while addressing specific knowledge gaps.

Figure 28 shows educational influences on collaboration importance perceptions, with technical education backgrounds valuing collaboration more highly. This indicates that cybersecurity collaboration strategies should leverage educational networks and professional associations to enhance cooperative security initiatives. The diploma holders' highest rating of collaboration importance likely reflects their practical experience with technical systems and recognition that cybersecurity requires coordinated efforts across different specializations. This group may have direct experience with the limitations of individual approaches to cybersecurity challenges. The undergraduate students' moderate ratings may reflect limited professional experience with collaborative cybersecurity initiatives. The progressive decrease in importance ratings from level 1 to 5 across all educational groups indicates general recognition of collaboration value, though with varying intensity. The postgraduate respondents' consistent moderate ratings suggest balanced appreciation for collaboration without extreme positions. These findings indicate that collaboration frameworks should be tailored to different educational backgrounds, with technical education groups serving as collaboration champions while other groups may require more persuasion about collaboration benefits. Professional development programs and educational partnerships may be effective channels for promoting cybersecurity collaboration.

Figure 29 shows urban populations' greater appreciation for cybersecurity collaboration, likely reflecting more complex organizational environments and interconnected systems. This suggests that collaboration frameworks should

be adapted to different settlement patterns and organizational structures. Urban residents' highest importance rating for collaboration may reflect their experience with complex digital ecosystems where multiple stakeholders must coordinate cybersecurity efforts. Urban areas typically have more diverse organizational structures and greater interdependence between systems. The semi-urban population's moderate collaboration importance ratings suggest growing recognition of collaboration needs as digital infrastructure develops. Rural residents' lower importance ratings may reflect simpler organizational structures and less complex digital environments where individual approaches to cybersecurity may seem more feasible. However, this perception may be changing as rural areas become more digitally connected and face increasingly sophisticated threats. The consistent decrease in importance ratings across levels indicates universal recognition of collaboration value, though with geographic variation in intensity. These findings suggest that collaboration strategies should be geographically differentiated, with urban areas receiving more sophisticated multi-stakeholder collaboration frameworks while rural areas benefit from simpler, community-based collaborative approaches.

Figure 30 shows declining collaboration importance perception with age, indicating potential generational barriers to cooperative cybersecurity initiatives. This suggests that collaboration strategies should address age-related preferences and communication styles to ensure inclusive participation across demographic groups. The 31-40 age group's highest importance rating for collaboration likely reflects their active participation in professional environments where collaborative approaches are common and their experience with complex digital systems requiring coordinated security efforts. This demographic may have the most direct experience with the benefits and challenges of cybersecurity collaboration. The declining importance ratings with advancing age may reflect several factors: preference for individual approaches to problem-solving, scepticism about collaborative effectiveness, or limited experience with modern collaborative tools and methods. Older demographics may have developed cybersecurity approaches during periods when individual solutions were more feasible. The 18-30 age group's moderate importance perception may reflect limited professional experience with collaborative cybersecurity initiatives despite familiarity with collaborative technologies. These findings suggest that collaboration strategies should be age-sensitive, with middle-aged groups serving as collaboration leaders while younger groups receive training on professional collaborative approaches and older groups receive support for participating in collaborative initiatives through familiar communication channels and methods.

CONCLUSIONS

The discourse surrounding cybersecurity in the Internet of Medical Things (IoMT) in Indian healthcare systems represents a fundamental challenge to technological security, patient safety, and the integration of advanced medical devices within the healthcare infrastructure. IoMT devices, characterized by interconnected medical equipment that continuously collect, transmit, and analyse patient data, continue to be deployed under a cybersecurity framework that lacks specialized protection protocols to address the unique vulnerabilities and threat landscapes of connected healthcare technologies. While the Indian healthcare system acknowledges the importance of digital health through various policy initiatives and technological adoption programs, these frameworks remain largely generic and unresponsive to the specific security needs posed by IoMT implementations. This disparity raises profound questions about India's preparedness to secure complex healthcare technologies, the readiness of healthcare institutions to implement comprehensive cybersecurity measures, and the extent to which Indian healthcare cybersecurity systems align with global standards of medical device security and patient data protection. The primary objective of this study was to evaluate the awareness, perception, and demographic variations in cybersecurity threat assessment among healthcare stakeholders regarding IoMT implementations and to assess the effectiveness of current technical and regulatory measures in mitigating cybersecurity risks in connected healthcare environments. The research was undertaken with the broader aim of investigating whether demographic factors significantly influence cybersecurity perception and mitigation strategies, and whether there is a need to introduce demographically-tailored cybersecurity frameworks for IoMT systems. At the heart of this exploration was the recognition of IoMT cybersecurity as a distinct and highly complex technological challenge that requires refined security methodologies grounded in demographic analysis and stakeholder-specific risk assessment. To fulfil these objectives, this research employed a quantitative methodology, focusing on stakeholder perspectives as a tool to gauge current levels of cybersecurity awareness, perceived threat landscapes, and demographic variations in security assessment. Data was collected using a structured survey comprising responses obtained through systematic sampling across diverse demographic groups in India. The demographic spread of respondents included various factors such as age, gender, educational qualification, and place of residence. Independent variables in the study included these demographic characteristics along with participants' exposure to cybersecurity training and IoMT technologies. Dependent variables consisted of perceived cybersecurity threats, assessment of mitigation effectiveness, trust factors in healthcare technology, and support for various cybersecurity improvement measures. This research reveals that software vulnerabilities constitute the most universally recognized primary cybersecurity threat across all demographic groups, transcending generational, educational, and geographic boundaries. This finding demonstrates widespread awareness of system weaknesses that pose fundamental risks to IoMT devices. The study

identifies a hierarchy of threats that includes ransomware attacks, which show particularly high concern among older adults (51-60 age group) and rural residents due to limited cybersecurity infrastructure and targeted exploitation campaigns. Data interception and unauthorized access emerge as consistently recognized threats across all demographics, indicating successful public awareness of transmission security risks. Additionally, device hardware and firmware vulnerabilities represent significant concerns, particularly among middle-aged professionals with system management experience and undergraduate-educated respondents with practical exposure to software systems. The research reveals significant gaps in current mitigation effectiveness, with substantial variation across demographic groups and geographic locations. Technical measures demonstrate limited effectiveness, evidenced by high reporting of cyberattack frequency among digitally engaged populations and significant geographical disparities in attack experiences. While postgraduate-educated individuals report fewer attacks, suggesting access to better cybersecurity practices, the overall pattern indicates uneven distribution of protective technical capabilities. Regulatory measures show insufficient framework development, with generational differences in institutional confidence and geographic disparities in regulatory support. Urban populations demonstrate preference for regulatory solutions due to greater institutional capacity, while rural areas show skepticism about regulatory relevance, creating substantial implementation challenges. The research reveals four critical findings in current IoMT cybersecurity that transcend professional demographics. First, there is widespread consensus across all educational levels, geographical locations, and age groups that current cybersecurity frameworks are fundamentally inadequate for IoMT security challenges, with software vulnerability management emerging as the most critical gap in protective protocols. Second, significant geographic disparities exist in cybersecurity capabilities, with semi-urban and rural areas facing disproportionate challenges in threat detection, incident response, and access to specialized cybersecurity resources, while rural jurisdictions show the strongest disagreement with current regulatory provisions. Third, professional experience creates a paradox where older practitioners demonstrate greater awareness of cybersecurity limitations and stronger confidence in advanced security measures' value, while younger professionals show more support for technical standardization and better recognition of the need for specialized approaches to IoMT security. Fourth, despite widespread recognition of cybersecurity's critical importance and overwhelming support for security awareness training, significant implementation barriers persist due to resource constraints, inadequate training programs, and the absence of standardized protocols that differentiate IoMT security from general healthcare cybersecurity. Based on these findings, comprehensive reforms must address both systemic inadequacies and demographic disparities through targeted interventions. Immediate implementation of specialized training modules for healthcare professionals in IoMT cybersecurity should be prioritized, accompanied by standardized protocols that clearly differentiate IoMT security requirements from general healthcare IT procedures, with particular emphasis on comprehensive vulnerability assessment frameworks. Geographic equity must be achieved through targeted resource allocation to semi-urban and rural healthcare facilities, including the establishment of regional cybersecurity centres of excellence that can provide specialized technical support and expert consultation to under-resourced areas. Healthcare cybersecurity regulations require fundamental amendments to incorporate flexible provisions specifically designed for complex IoMT environments, allowing healthcare institutions greater discretion in handling cybersecurity incidents while ensuring adequate monitoring and response systems that address the unique security and operational requirements of connected medical devices. Finally, a national IoMT security registry and dedicated cybersecurity units should be established to create systematic approaches for tracking patterns in cyber threats, while professional development programs must be standardized across all educational levels to ensure consistent competency in cybersecurity techniques and modern protective methods. In conclusion, this study affirms that the integration of comprehensive cybersecurity measures into IoMT implementations in Indian healthcare systems is not merely a technical upgrade, but a fundamental institutional and societal imperative. As India continues to evolve in its healthcare digitization and technology adoption, it must prioritize the security dimensions of connected medical devices to effectively confront the growing complexity of cyber threats in healthcare environments. Recognizing IoMT cybersecurity as a demographically complex challenge—and comprehensive security frameworks as legitimate healthcare necessities—marks a critical step toward a more responsive, analytical, and scientifically informed healthcare system. This transformation will not only enhance healthcare security capacity but also uphold the ideals of patient safety, data protection, and institutional preparedness in the face of evolving cyber threats. The convergence of demographic diversity, threat awareness, and cybersecurity readiness must be systematically addressed to ensure that IoMT technologies fulfil their promise of improved healthcare delivery while maintaining the highest standards of security and patient protection.

Limitations

The research recognizes its limitations, particularly the focus on perception-based data and potential regional variations in cybersecurity infrastructure. However, these limitations offer valuable direction for future research. The future scope is that further studies could expand the sample to include healthcare administrators, cybersecurity professionals, technology vendors, and policy makers to explore systemic readiness across the healthcare technology ecosystem.

Additionally, region-wise studies could reveal how infrastructure, training, and resource variations influence cybersecurity capacity across different states and healthcare delivery models. Qualitative interviews with experienced healthcare cybersecurity professionals and IoMT specialists would also offer in-depth perspectives on ground-level challenges and implementation solutions. Comparative studies with IoMT cybersecurity practices in countries with advanced healthcare digitization such as the United States, European Union, and Singapore could provide benchmarking models for Indian adaptation and policy reform. Longitudinal studies tracking cybersecurity awareness evolution over time would help understand the dynamic nature of threat perception and mitigation effectiveness. Furthermore, experimental studies examining the effectiveness of different cybersecurity training methodologies across demographic groups could inform the development of targeted educational programs.

REFERENCES

[1] Joyia, G.J. *et al.* "Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain." *Journal of Communications*, vol. 12, no. 4, 2017, pp. 240–247.

[2] Gatouillat, A. *et al.* "Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine." *IEEE Internet of Things Journal*, vol. 5, no. 5, 2018, pp. 3810–3822. https://doi.org/10.1109/JIOT.2018.2832538.

[3] Hatzivasilis, G. *et al.* "Review of security and privacy for the Internet of Medical Things (IoMT)." *Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2019, pp. 457–464. https://doi.org/10.1109/DCOSS.2019.00088.

[4] Nkomo, D. and R. Brown. "Hybrid cyber security framework for the Internet of Medical Things." *Blockchain and Clinical Trial: Securing Patient Data*, Springer International Publishing, 2019, pp. 211–229. https://doi.org/10.1007/978-3-319-98911-1_11.

[5] Vishnu, S. *et al.* "Internet of medical things (IoMT) — An overview." *Proceedings of the 2020 5th International Conference on Devices, Circuits and Systems (ICDCS)*, 2020, pp. 101–104. https://doi.org/10.1109/ICDCS48721.2020.00028.

[6] Yaacoub, J.P.A. *et al.* "Securing Internet of Medical Things systems: Limitations, issues and recommendations." *Future Generation Computer Systems*, vol. 105, 2020, pp. 581–606. https://doi.org/10.1016/j.future.2019.12.040.

[7] Thomasian, N.M. and E.Y. Adashi. "Cybersecurity in the internet of medical things." *Health Policy and Technology*, vol. 10, no. 3, 2021, pp. 100549. https://doi.org/10.1016/j.hlpt.2021.100549.

[8] Saheed, Y.K. and M.O. Arowolo. "Efficient cyber attack detection on the Internet of Medical Things-smart environment based on deep recurrent neural network and machine learning algorithms." *IEEE Access*, vol. 9, 2021, pp. 161546–161554. https://doi.org/10.1109/ACCESS.2021.3130631.

[9] Elsayeh, M. *et al.* "Cybersecurity architecture for the internet of medical things and connected devices using blockchain." *Biomedical Engineering: Applications, Basis and Communications*, vol. 33, no. 2, 2021, pp. 2150013. https://doi.org/10.4015/S1016237221500130.

[10] Razdan, S. and S. Sharma. "Internet of medical things (IoMT): Overview, emerging technologies, and case studies." *IETE Technical Review*, vol. 39, no. 4, 2022, pp. 775–788. https://doi.org/10.1080/02564602.2020.1861383.

[11] Kakhi, K. *et al.* "The internet of medical things and artificial intelligence: Trends, challenges, and opportunities." *Biocybernetics and Biomedical Engineering*, vol. 42, no. 3, 2022, pp. 749–771. https://doi.org/10.1016/j.bbe.2022.06.003.

[12] Hasan, M.K. *et al.* "A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things." *IET Communications*, vol. 16, no. 5, 2022, pp. 421–432. https://doi.org/10.1049/cmu2.12263.

[13] Huang, C. *et al.* "Internet of medical things: A systematic review." *Neurocomputing*, vol. 557, 2023, pp. 126719. https://doi.org/10.1016/j.neucom.2023.126719.

[14] Ameen, A.H. *et al.* "Dimensions of artificial intelligence techniques, blockchain, and cyber security in the Internet of medical things: Opportunities, challenges, and future directions." *Journal of Intelligent Systems*, vol. 32, no. 1, 2023, pp. 20220267. https://doi.org/10.1515/jisys-2022-0267.

[15] Alkatheiri, M.S. and A.S. Alghamdi. "Blockchain-assisted cybersecurity for the internet of medical things in the healthcare industry." *Electronics*, vol. 12, no. 8, 2023, pp. 1801. https://doi.org/10.3390/electronics12081801.

[16] Yazid, A. "Cybersecurity and privacy issues in the Internet of medical things (IoMT)." *Eigenpub Review of Science and Technology*, vol. 7, no. 1, 2023, pp. 1–21.

[17] Vijayakumar, K.P. *et al.* "Enhanced cyber attack detection process for Internet of Health Things (IoHT) devices using deep neural network." *Processes*, vol. 11, no. 4, 2023, pp. 1072. https://doi.org/10.3390/pr11041072.

[18] Bughio, K.S. *et al.* "Developing a novel ontology for cybersecurity in internet of medical things-enabled remote patient monitoring." *Sensors*, vol. 24, no. 9, 2024, pp. 2804. https://doi.org/10.3390/s24092804.

[19] Ksibi, S. *et al.* "MLRA-Sec: An adaptive and intelligent cyber-security-assessment model for Internet of Medical Things (IoMT)." *International Journal of Information Security*, vol. 24, no. 1, 2025, pp. 21. https://doi.org/10.1007/s10207-024-00866-2.

[20] Khan, A.A. *et al.* "BDLT-IoMT — A novel architecture: SVM machine learning for robust and secure data processing in Internet of Medical Things with blockchain cybersecurity." *The Journal of Supercomputing*, vol. 81, no. 1, 2025, pp. 271. https://doi.org/10.1007/s11227-024-06153-y.

[21] Selvamuthu, C.M. *et al.* "Perceptions of health insurance schemes and their role in reducing healthcare disparities across Asian populations: Insights into access, equity and policy." *Journal of Pioneering Medical Sciences*, vol. 14, no. 1, 2025, pp. 38–53. https://doi.org/10.47310/jpms2025140106.

[22] Gopalan, K.R. *et al.* "Contaminated consumption: Unveiling the health hazards of food adulteration and its profound impact on public health in India." *Journal of Pioneering Medical Sciences*, vol. 13, no. 7, 2025, pp. 75–88. https://doi.org/10.47310/jpms2024130713.

[23] Gopalan, K.R. *et al.* "A study on the legal complexities surrounding medical negligence in telemedicine in India." *Journal of Pioneering Medical Sciences*, vol. 14, no. 3, 2025, pp. 62–75. https://doi.org/10.47310/jpms2025140307.

[24] Vandana, V. *et al.* "Music therapy as a viable alternative medicine for improving psychological well-being." *Journal of Pioneering Medical Sciences*, vol. 14, no. 3, 2025, pp. 7–20. https://doi.org/10.47310/jpms2025140302.